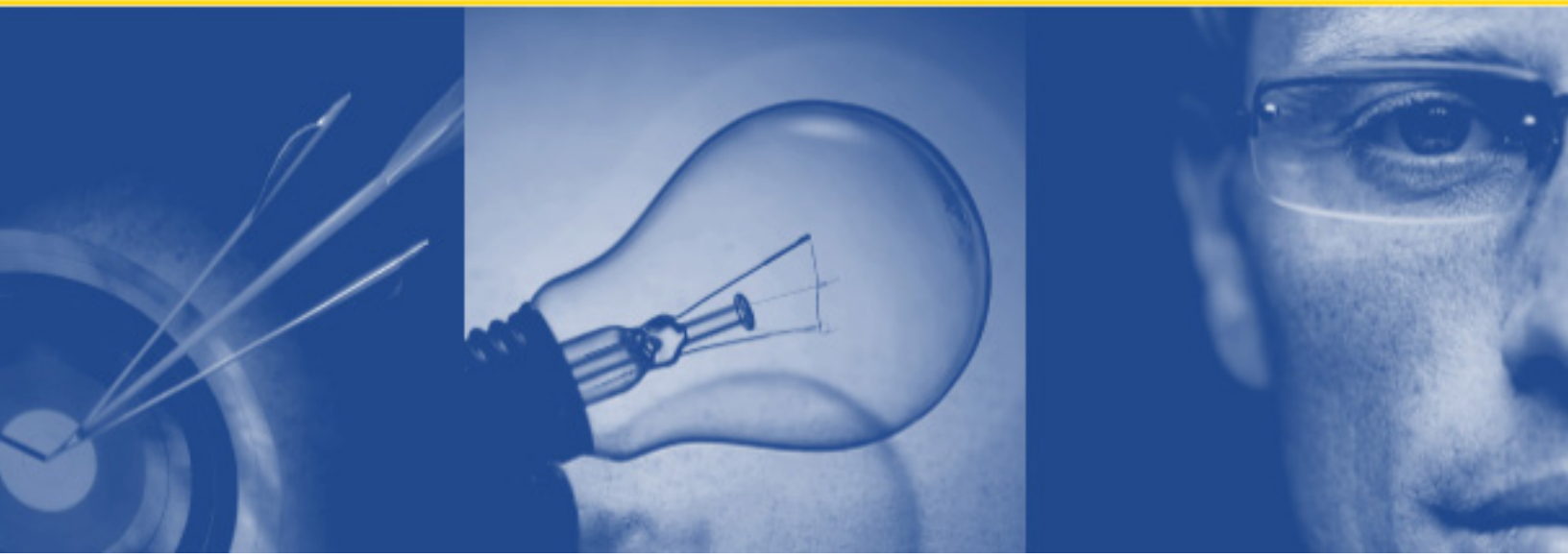
QUEST SOFTWARE®
Simplicity At Work™

Quest® One Identity Manager 5.0

Identity Management



© 2011 Quest Software, Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters

LEGAL Dept

5 Polaris Way

Aliso Viejo, CA 92656

email: legal@quest.com

Refer to our Web site (www.quest.com) for regional and international office information.

Patents

This product includes patent pending technology.

Trademarks

Quest, Quest Software, the Quest Software logo and Quest One Identity Manager are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. For a complete list of Quest Software's trademarks, please see http://www.quest.com/legal/trademarks.aspx. Other trademarks and registered trademarks are property of their respective owners.

Third Party Contributions

Quest One Identity Manager contains some third party components (listed below). Copies of their licenses may be found at http://www.quest.com/legal/third-party-licenses.aspx.

COMPONENT	LICENSE OR ACKNOWLEDGEMENT
ExplorerCanvas Release 3	Copyright © 2006 Google Inc. Apache 2.0 License.
MochiKit 1.4.2	Copyright © 2005 Bob Ippolito. All rights reserved. MIT License.
Mono.Security 2.0.3600.1	Copyright © 2004 Novell, Inc. (http://www.novell.com). MIT License.
Novell.Directory.LDAP 2.1.9.0	Copyright © 2003 Novell, Inc. (http://www.novell.com). MIT License.
PlotKit 0.9.1	Copyright © 2006 Alastair Tse. BSD Simple License.

Quest One Identity Manager - Identity Management

Updated - 18.5.11

Software Version - 5.0.1

CONTENTS

CHAPTER 1
ABOUT THIS GUIDE

QUEST® ONE IDENTITY MANAGER 20
INTENDED AUDIENCE 20
DOCUMENTATION MANUALS 20
CONVENTIONS 22
ABOUT QUEST SOFTWARE, INC. 22
CONTACTING QUEST SOFTWARE, INC. 22
CONTACTING QUEST SUPPORT 23

CHAPTER 2
EMPLOYEES AND USER ACCOUNTS

INTRODUCTION 26
BASIC MECHANISMS FOR EMPLOYEE AND USER ACCOUNT ADMINISTRATION 26
MANUAL HANDLING OF USER ACCOUNTS 27
HANDLING USER ACCOUNTS DURING SYNCHRONIZATION 28
ASSIGNING EMPLOYEES AUTOMATICALLY TO EXISTING USER ACCOUNTS 28
HANDLING USER ACCOUNTS WITH USER ACCOUNT RESOURCES 28
EMPLOYEE AND USER ACCOUNT ADMINISTRATION 29
HANDLING EMPLOYEES AND USER ACCOUNTS 30
CENTRAL USER ACCOUNT 31
DEFAULT EMAIL ADDRESS 31
DETERMINING THE IT OPERATING DATA FOR AN EMPLOYEE'S USER ACCOUNT 32
DETERMINING IT OPERATING DATA 33
ACTIVATING IT OPERATING DATA ASSIGNMENTS 34
DETERMINING DEPARTMENTS, COST CENTER, LOCATIONS AND BUSINESS ROLES 34
SPECIFYING THE IT OPERATING DATA DEFAULT VALUES 35
TESTING DEFAULT VALUES 36
CREATING USER ACCOUNTS WITH USER ACCOUNT RESOURCES 37
USING SEVERAL USER ACCOUNT RESOURCES WITHIN A TARGET SYSTEM 38
AUTOMATIC ASSIGNMENT OF EMPLOYEES TO USER ACCOUNTS 40
CONFIGURING AUTOMATIC EMPLOYEE ASSIGNMENT 41
MAPPING PROPERTIES DURING AUTOMATIC EMPLOYEE ASSIGNMENT 42
CHANGING EMPLOYEE MASTER DATA 43
HANDLING DISABLING AND DELETION OF EMPLOYEES AND USER ACCOUNTS 44
TEMPORARY DEACTIVATION OF AN EMPLOYEE 44
PERMANENT DEACTIVATION OF AN EMPLOYEE 44
DEFERRED DELETION OF AN EMPLOYEE 45
DISABLING AND DELETING THROUGH USER ACCOUNT RESOURCES 45
ENTERING EMPLOYEE MASTER DATA 46
EMPLOYEE MASTER DATA 47
ORGANIZATIONAL EMPLOYEE MASTER DATA 49
ADDRESS DATA 51
MISCELLANEOUS EMPLOYEE MASTER DATA 53
USER DEFINED EMPLOYEE MASTER DATA 55
ADDITIONAL TASKS FOR MANAGING EMPLOYEES 55

Mapping Multiple Employee Identities 58

Chapter 3
The Identity Manager Roles Model

Introduction 62
The Identity Manager Application Roles 62
How to Edit Identity Manager Application Roles 67
Assigning Application Roles after Initial Database Migration 67
How to Edit Master Data 68
General Master Data 68
User Defined Master Data 69
Additional Tasks for Managing Application Roles 69
Assign Employees 69
How to Edit Conflicting Application Roles 70
Identity Manager Application Roles for Target System Adminstration 70

Chapter 4
Company Structures as Roles in the Identity Manager

Introduction 74
Basics for Creating Roles 74
Direction of Inheritance within a Hierarchical Role Structure 74
Discontinuing Inheritance 75
Possible Assignment Types 76
Direct Assignment 76
Indirect Assignment 76
Primary Assignment 77
Secondary Assignment 78
Assigning Company Resources through Roles 78
Sorting Employees into Roles 78
Specifying the Direction of Inheritance for Roles 79
Using Roles to Limit Inheritance 79
Possible Company Resource Assignments via Roles 79
Inheritance Exclusion 80
Inheriting Group Memberships Based on Categories 82
Basic Data for Constructing Roles 84
Role Classes 84
Role Types 85
Functional Areas 86
Application Roles 87
Business Roles 88
Reports about Business Roles 89
Departments 92
Cost Centers 94
Locations 95
Additional Tasks for Managing Roles 96
Setting Up IT Operating Data 99
Working with Dynamic Roles 100
Setting Up Dynamic Roles 100

Calculating Role Memberships 102
Setting Up a Scheduled Task to Calculate Dynamic Roles 103
Calculating Execution Times 104
Chapter 5
Resource Administration
Introduction 106
Resources 106
Base Data for Resources 106
Resource Types 106
Processing Status 107
Editing Resources 108
Resource Packages 109
Additional Tasks for Managing Resources 109
Assign System Roles 109
Assign Business Roles and Organizations 110
Assign to Employees 110
Add Resources to the IT Shop 110
Assign Extended Properties to Resources 110
Reports about Resources 110
Mapping a Business Role to a Resource 112
System Roles 114
System Role Types 115
Editing System roles 115
Additional Tasks for Managing System Roles 116
Assign Business Roles and Organizations 117
Assign to Employees 117
Add to IT Shop 117
Assign Extended Properties 117
Assign Company Resources 117
Assign System roles 118
Edit Conflicting System Roles 118
Reports about System Roles 118
System Entitlements, Groups, Applications 121
Chapter 6
Managing Applications
Introduction 124
Editing Applications 124
Basic Data for Setting Up Applications 124
Setting Up Applications 124
General Master Data for an Application 125
Extended Master Data for an Application 125
Persons in Charge 126
Application Inventory Data 126
User Defined Master Data 126
Additional Tasks for Managing Applications 126
Deleting Applications 127

Setting Up and Sharing Application Packages 127
Installation Order and Physical Software Dependencies 127
Editing Logical Dependencies 128
Editing Physical Dependencies 128
Editing Software Installation Prerequisites 128
Editing Self-Excluding Software 129

Chapter 7
The Unified Namespace

Introduction 132
Unified Namespace Basics 132
Advice for Enabling a Target System in the Identity Manager 134
Advice for Full Management of Target Systems in the Identity Manager 134
Unified Namespace Configuration 135
Setting Up Target System Types in the Unified Namespace 135
Reports about Target System Types 137
Target System Manager 139
Unified Namespace Permissions Controls 140
Permissions Control General Master Data 140
Permissions Controls User Defined Master Data 140
Additional Tasks for Permissions Controls 140
Container Structures in the Unified Namespace 141
Reports about Container Structures 142
User Accounts in the Unified Namespace 144
Entering Master Data for Unified Namespace User Accounts 145
Additional Tasks for Managing Unified Namespace User Accounts 148
Assign System Entitlements directly to a Unified Namespace User Account . . 148
Assign Extended Properties to Unified Namespace User Accounts 148
Managing Unified Namespace User Accounts with User Account Resources 148
Setting Up a User Account Resource 149
Manage Level for Handling Unified Namespace User Accounts 152
Deleting User Account Resources 153
System Entitlements in the Unified Namespace 154
Additional Tasks for Managing System Entitlements 156
Assign Business Roles and Organizations 156
Assign System Roles 156
Assign User Accounts 156
Assign System Entitlements 157
Specify Inheritance Exclusion 157
Add System Entitlements to the IT Shop 157
Assign Extended Properties to System Entitlements 157
Reports about System Entitlements 158

Chapter 8
Data Synchronization in Identity Manager

Introduction 162
Synchronisation by Identity Manager 162
Loading Target System Schema and Mapping Rules 163
How to Configure Synchronization 163

Existing Configurations 164
Current Configuration 165
Additional Settings 167
Object Type, Assignment and Synchronization Behavior 168
Synchronized Object Types and Assignments 168
Filter 169
Synchronization Behavior for Selected Objects 170
Affects of the Master Definition 171
How to Speed up Synchronization 174
How to Define a Mapping 175
Logging Synchronization Errors 176
Synchronization Analysis 176
Synchronisation Post Processing 177
Synchronization Data Display 179
Customizing Mapping rules 180
Basics for Customizing Mapping Rules 180
Mapping Editor Functions 181
Editing a Mapping Rule 183
Mapping Target System Schema to the Database Schema 185
Mapping Object Relations 186
Adding elements to the Mapping Definition 186
Deleting Elements from the Mapping Definition 187
Editing Object Types 187
Formulating the Mapping Definition as an SQL Query 188
Defining Dependencies 190
Editing Assignments 191
Specifying the Data Master for Object Properties 192
Modifying the Column Mapping 192
Special Cases of Synchronization 194
Editing Table Relations 194
Synchronization Server Administration 196

Chapter 9
Managing an Active Directory Environment

Introduction 202
Setting Up Active Directory Synchronization 202
Installation and Configuration of the Active Directory Synchronization Server . . 202
Identity Manager Service Access Rights Necessary for Synchronization with Active Directory Service 203
Setting Up the Identity Manager Database for Synchronization with an Active Directory Environment 204
Using the Target System Wizard for Setting Up Synchronization 205
Declaring the Active Directory Synchronization Server 205
Setting Up an Active Directory Domain 206
General Master Data for an Active Directory Domain 206
Specifying User Account Policy 208
Customizing Sychronization Data 209

Active Directory Specific Master Data 210
Login Data 211
Configuration of Extended Properties for an Active Directory Domain 212
Trusted Domains 212
Reports about Active Directory Domains 213
Configuring Active Directory Domain Synchronization 215
Configuration Parameters for Synchronization with an Active Directory Environment 216
Special features of Active Directory Domain Synchronization Configuration 217
Speeding Up Synchronization by Including an Update Sequence Number 219
Basic Configuration Data 219
Active Directory Container Structures 219
Setting Up Active Directory Containers 220
Addtional Tasks for Managing Active Directory Containers 221
Active Directory User Accounts 221
Entering Active Directory User Account Master Data 222
General Master Data for an Active Directory User Account 222
Password Data for Active Directory 225
Profile and Home Directories 227
Active Directory User Account Login Data 229
Remote Access Service Dial-in Permissions 230
Connection Data for a Terminal Server 231
Further Identification Data 233
Contact Data for an Active Directory User Account 233
Additional Tasks for Managing Active Directory User Accounts 234
Managing Active Directory User Accounts with User Account Resources 234
Creating a User Account Resource for an Active Directory Domain 235
Manage Levels for Handling Active Directory User Accounts 237
Deleting and Restoring Active Directory User Accounts 239
Active Directory Contacts 241
Entering Master Data for Active Directory Contacts 241
General Master Data for Active Directory Contacts 241
Contact Data for an Active Directory Contact 243
Further Identification Data 244
Additional Tasks for Managing Active Directory Contacts 244
Active Directory Groups 245
Entering Master Data for Active Directory Groups 246
Validity of Group Memberships 247
Additional Tasks for Managing Active Directory Groups 252
Reports about Active Directory Groups 253
Account Policies for Active Directory Domains 255
Entering Account Policies 256
General Master Data for an Account Policy 256
How to Define a Policy 257
Assigning Account Policies to Users 258
Setting Up Synchronization with a Microsoft Exchange Environment 258
Installation and Configuration of a Microsoft Exchange Synchronization Server . 258

Necessary Identity Manager Service Access Rights to Synchronize with a Microsoft Exchange Environment . . . 259
Setting up the Identity Manager Database for Synchronization with a Microsoft Exchange Environment. . . . 260
Declaring the Microsoft Exchange Synchronization Server . . . 261
Determining the Valid Data Synchronization Server . . . 262
Active Directory Domain Extended Master Data for Synchronizing with Microsoft Exchange . . . 263
How to Configure Synchronization with a Microsoft Exchange Environment . . 264
Configuration Parameters for Synchronizing with Microsoft Exchange . . . 264
Special Features of Microsoft Exchange Synchronization Configuration . . . 265
Microsoft Exchange Structure . . . 267
Graphical Representation of the Microsoft Exchange Structure in the Identity Manager . . . 267
Microsoft Exchange Organization . . . 267
Microsoft Exchange Administrative Groups . . . 268
Microsoft Exchange Storage Groups . . . 269
Microsoft Exchange Mailbox Store . . . 270
Microsoft Exchange Public Folder. . . . 271
Microsoft Exchange Address Lists . . . 273
Policies for Mobile Email Queries . . . 274
Folder Administration Policies . . . 276
Policies for Shares . . . 276
Microsoft Exchange Recipients . . . 276
Setting Up Microsoft Exchange Mailboxes . . . 277
Supported Mailbox types as from Microsoft Exchange Server 2007 . . . 277
Enabling a Microsoft Exchange Mailbox . . . 277
Microsoft Exchange Mailbox Master Data . . . 278
Limits for a Microsoft Exchange Mailbox . . . 281
Booking Resources . . . 282
Extended Data for a Microsoft Exchange Mailbox . . . 283
Additional Tasks for Handling Microsoft Exchange Mailboxes . . . 283
Administration of Microsoft Exchange Mailboxes via User Account Resources . 284
Creating a User Account Resource for a Microsoft Exchange Environment. . 284
Specifying Manage Levels for Handling Microsoft Exchange Mailboxes . . . 287
Setting Up Mail-enabled User and Contacts . . . 288
Enabling a Mail-enabled User Account or Contact . . . 288
Master Data for Email Addressing . . . 289
Extended Data for Mail-Enabled Recipients . . . 290
Additional Tasks for Managing Mail-enabled Recipients . . . 290
Mail-enabled Groups . . . 291
Enabling and Disabling a Distribution Group . . . 291
Email Addressing Master Data . . . 291
Extensions for Dynamic Distributions Groups. . . . 292
Approving Membership in Distribution Groups . . . 293
Moderated Distribution Group Extensions . . . 293
Additional Tasks for Managing Distribution Groups . . . 293
Chapter 10

Managing a Lotus Notes Environment

Introduction 296
Lotus Notes Synchronization Procedure 296
Setting Up Lotus Notes Sychronization 298
Installation and Configuration of a Gateway Server 298
Lotus Notes Client Installation 299
Preparing User Accounts for Synchronization 300
How to Copy the Lotus Notes Certificate 301
Setting up an Archive Database for backing Up Employee Documents 302
Identity Manager Services Installation and Configuration 302
Customizing VINotes.INI 303
viAgentsDB.nsf Signature 303
The Identity Manager Database Synchronization Setup for Lotus Notes 304
Target System Wizard for the Identity Manager Database Synchronization with Lotus Notes 305
Declaring the Gateway Server 306
Lotus Notes Domain Setup in the Identity Manager Database 306
General Master Data for a Lotus Notes Domain 307
How to Customize Data Synchronization 308
Declaring the Domino Servers in the Identity Manager Database 309
Testing Domino Server Functional Efficiency 310
Accelerating Synchronisation 310
Using AdminP Request for Handling Lotus Notes Processes 312
Synchronizing AdminP Procedures 312
Accelerating Handling of AdminP Requests 313
Automated Confirmation of AdminP Requests 313
Basic Configuration Data 313
Lotus Notes Certificate 314
Lotus Notes Templates 315
Lotus Notes User Account 315
Entering Lotus Notes User Account Master Data 316
General Master Data for a Lotus Notes User Account 317
Lotus Notes User Account Account Email System 319
Lotus Notes User Account Address Data 320
Additional Master Data for a Lotus Notes User Account 320
Administrative Data for a Lotus Notes User Account 322
Managing Lotus Notes User Accounts with User Resource Accounts 324
Creating a User Resource Account for a Lotus Notes Domain 325
Specifying Rules for Handling Lotus Notes User Accounts 327
Restoring User IDs 328
Locking and Unlocking Lotus Notes User Accounts 329
Deleting Lotus Notes User Accounts 330
Lotus Notes Groups 330
Lock Groups in the Identity Manager 332
Additional Tasks for Managing Lotus Notes Groups 332
Deleting Lotus Notes Groups 334
Mail-In Databases 334

Lotus Notes Servers 335
General Master Data for Lotus Notes Servers 335
Location Data for Lotus Notes Servers 337
Security Settings for Lotus Notes Servers 338
Server Permissions Settings 339
Server Restriction Settings 341
Additional Tasks for Managing Lotus Notes Servers 342

Chapter 11
Managing an SAP R/3 Environment

Introduction 344
Setting Up SAP R/3 Synchronization 344
SAP Synchronization Server Installation and Configuration 344
Installing the Identity Manager Business Application Programing Interface . 345
Permissions Required for SAP R/3 Synchronisation 346
Setting Up the Identity Manager database for SAP R/3 Synchronisation 347
Target System Wizard for Identity Manager Database Synchronization with SAP R/3 347
Declaring the Synchronization Server 348
System Setup in the Identity Manager Database 349
System Reporting 350
Client Synchronization Setup 352
General Master Data for a Client 352
Specifying Categories 354
Customizing Data Synchronization 354
Reports about Clients 355
Configuring Client Synchronization 357
Configuration Parameters for Synchronization with an SAP R/3 Environment . . 358
Special Features of Client Synchronization Configuration 358
Special Features of Synchronizing with a CUA Central System 360
Restricting Synchronization Objects Using User Permissions 360
Basic Configuration Data 361
Managing User Accounts 361
Basic Data for User Account Administration 362
User Account Types 362
Types for External Identification 363
Licenses 363
SAP Printers 364
SAP Cost Centers 364
SAP Start Menus 364
SAP Company Addresses 364
SAP Login Language 365
Entering User Account Master Data 365
General Master Data for a User Account 366
User Account Login Data 369
Contact Data for a User Account 371

Fixed Values for a User Account 372
Inventory Data 372
SNC Data for a user account 373
System Assignment for CUA 373
Additional Tasks for Managing user accounts. 373
Assign Extended Properties 373
Assign Groups, Roles, Profiles and Structural Profiles 373
Lock Account 374
Managing user accounts with User Account Resources 374
Creating a User Account Resource for an Client. 375
Specifying Manage Levels for Handling User Accounts. 377
Deleting User Account Resources 379
Deleting user accounts 380
Automatically Adding and Deleting user accounts by Changing Group Memberships 380
CUA Implementation Features 381
Entering External User Identifiers for a User Account 382
Groups, Profiles and Roles Administration 383
Additional Tasks for Managing Groups 385
Assign Business Roles and Organizations 385
Adding to the IT Shop 386
Assign user accounts 386
Assign System Roles 386
Specify Inheritance Exclusion 386
Assign Extended Properties for Groups, Roles and Profiles 386
Show Authorizations and Authorization Objects 387
Special Assignment Cases for User Accounts and Groups, Profiles and Roles. . 387
Reports About System Entitlements 388
Compiling Products 390
Additional Tasks for Managing Products 391
Managing Structural Profiles 391
Entering General Master Data for Structural Profiles 392
Additional Tasks for Structural Profiles. 393
Assign Business Roles and Organizations 393
Add to IT Shop 393
Specify Inheritance Exclusion 394
Assign User Accounts 394
Providing System Measurement Data 394
Graphical Representation of Measurement Data. 394
Determining User Account Rating 396
Transfering Calculated Licenses 398

Chapter 12
Managing Generic Target Systems

Introduction 400
Special Cases for Implementing Synchronization between the Identity Manager Database and the LDAP Directory 400
Setting Up LDAP Directory Synchronization. 401
Installation and Configuration of the LDAP Synchronization Servers 401

The Identity Manager Database Setup for Synchronization with an LDAP Directory 402
Declaring the LDAP Synchronization Server 403
Declaring the LDAP Store Server 403
Setting Up an LDAP Domain 403
General Master Data for an LDAP Domain 404
User Account Policy 405
Customizing Synchronization Data 405
LDAP Specific Master data 406
Login Data 407
Accelerating Synchronization 407
LDAP Container Structures 407
LDAP User Accounts 409
Entering LDAP User Account Master Data 409
General Master Data for a User Account 409
Login Data for a User Account 411
Additional Master Data for a User Account 411
Additional Tasks for Managing User Accounts 411
Managing User Account through User Account Resources 412
Creating a User Account Resource for a Domain 413
Specifying Manage Levels for Handling User Accounts 415
Deleting User Accounts 417
LDAP Groups 418
Additional Tasks for Managing Groups 419
Deleting Groups 420

Chapter 13
Rule Compliance in the Identity Manager

Introduction 422
Setting up a Rule Base 423
Base Data for Setting up Rules 423
Setting Up Extended Properties 424
Specifying Scoped Boundaries 426
Risk Evaluation 427
Setting up Mitigating Controls 428
Additional Tasks for Mitigating Controls 429
Rule Violations 429
Setting up and Editing Rules 430
General Master Data for a Rule 431
Maintaining the Rule Supervisor and Exception Approvers 432
Rule Assessment Criterion 434
Extended Rule Input 434
Comparing a Rule Working Copy with the Original 435
IT Shop Properties for a Rule 436
Additional Tasks for Rules 437
Creating Rule Conditions 439
Basics for Using the Rule Editor 440

Specifying the Affected Employee Group 442
Specifying Affected Assignments 443
A Simple Rule Example 444
Creating Advanced Rule Conditions 445
Rule Conditions for SAP Functions 447
Rule condition as SQL query 448
Deleting Rule 448
Rule Checking 449
Checking a Rule 449
Rule Checking 450
Which Employees Violate a Certain Rule? 450
Which Rules are Violated by a Certain Employees? 451
Reports about Rule Violations 452
Granting Exception Approval 454
Determining Potential Rule Violations 456
SAP Functions 456
Prerequisites 458
Base Data for SAP Functions 459
SAP Function Categories 460
Setting Up SAP Functions 460
General Master Data for an SAP Function 461
Additonal Tasks for Working Copies 462
Addition Tasks for Function Definitions 465
Define Function Instances 466
Additional Tasks for Function Instances 467
Adding Variable Sets 467
Additional Tasks for Variable Sets 469
Plugins for SAP Functions 469
Export Function Definitions 469
Import Function Definitions 469

Chapter 14
Attestation and Recertification

Introduction 472
Defining Attestation Instances 472
Entering Base Data 472
Attestation Procedures 473
Schedules 474
Attestation Approval Policies and Workflows 475
Attestation Approval Procedures 475
Setting Up Attestation Policies 479
Additional Tasks for Attestation Policies 480
Monitoring Attestation Instances 481
Additional tasks for Attestation Instances 482
Attestation Instance Overview 482
Approval Sequence 482
Attestation History 482

Glossary 483

INDEX **497**

1

About this Guide

- Quest® One Identity Manager
- Intended Audience
- Conventions
- About Quest Software, Inc.

Quest® One Identity Manager

Quest One Identity Manager streamlines the process of managing user identities, access privileges and security enterprise wide. It empowers IAM to be driven by business needs, not IT capabilities. Quest One Identity Manager is based on an automation-optimized architecture that addresses major IAM challenges at a fraction of the complexity, time, or expense of "traditional" solutions.

Intended Audience

This manual deals with the Identity Management and User Provisioning components that are integrated into the Identity Manager. The aim is to provide company employees with the necessary company resources that they need to enable them to work effectively with respect to their job functions.

You will discover how to manage employees and their user accounts using the Identity Manager and how to represent their company structures and resources within the Identity Manager. Different mechanisms are described for supplying employees with user accounts in the connected target systems.

Furthermore, the methods that the Identity Manager uses for data synchronization are explained along with descriptions of the necessary configuration settings for synchronizing the Identity Manager database with each target system.

The Manual describes how you implement company specific IT policies, deal with rule violations and attest to the validity of rules, access permissions or assignments.You will discover how to define and monitor rules within an Identity Audit framework, how to deal with rule violations and automate or manually initiate corrective measures for them. The attestation function allows you to define objects and conditions that you want to attest. You can execute attestation instances either automatically or manually.

This manual is intended for system administrators, consultants, analysts, and any other IT professionals using the product.

This manual describes the default user functionality of the Identity Manager. It is possible that not all the functions described here are available to you. This depends on your system configuration and permissions.

Documentation Manuals

Identity Manager documentation includes the following manuals as well as the ”Identity Management“ Manual. They can be found on the distribution CD in the directory ...\Quest One Identity Manager\Documentation.

Getting Started

The main components of the Getting Started Manual are:

- Installation prerequisites
- Installation and updates of Identity Manager administration tools
- Identity Manager database setup
- Configuration of administration workdesks

- Configuration of server for accessing the database
- Overview of Identity Manager administration and configuration tools
- User interface for the main Identity Manager tools

Identity Management

The main components of the Identity Management Manual are:

- Identity Management and User Provisioning with Identity Manager
- Complying to and monitoring regulatory requirements using Identity Audit

Process Orchestration

The main components of the Process Orchestration Manual are:

- Monitoring process handling
- Controlling process handling
- Troubleshooting

Configuration

The main components of the Configuration manual are:

- Identity Manager software architecture
- Configuration of Identity Manager data models
- System permissions configuration
- User interface configuration
- Script processing
- Creating reports
- Data transport
- System configuration parameters
- Identity Manager inheritance mechanism
- Service provisioning using Service Provisioning Markup Language (SPML)
- Provider mode

IT Shop

The main components of the IT Shop manual are:

- IT Shop for authorized employees to supply themselves with company resources.
- Developement of approval policies and workflows

Web Designer Reference

The main sections in the Web Designer References are:

- IT Shops Developement and Configuration with the Web Designer

Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

ELEMENT	CONVENTION
<>	Identifies the user interface buttons and menu entries or keystrokes on the keyboard.
Blue Text	Indicates a cross-reference.
	Used to highlight additional information pertinent to the process being described.
	Used to provide Best Practice information. A best practice details the recommended course of action for the best result.
	Used to highlight processes that should be performed with care.
+	A plus sign between two keystrokes means that you must press them at the same time.

About Quest Software, Inc.

Quest Software simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to www.quest.com.

Contacting Quest Software, Inc.

Email	info@quest.com
Mail	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to SupportLink, our self-service portal. Visit SupportLink at http://support.quest.com/.

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at http://support.quest.com/pdfs/Global Support Guide.pdf.

2

Employees and User Accounts

- Introduction
- Basic Mechanisms for Employee and User Account Administration
- Handling Employees and User Accounts
- Entering Employee Master Data

Introduction

The main component of the Identity Manager maps employees and their basic information and user accounts to each of the target systems. Because requirements vary between companies, the Identity Manager offers methods for supplying user accounts to employees:

- Employee and user account data in the Identity Manager can be manually entered and assigned to each other.
- When user accounts are inserted in the Identity Manager, they can be automatically assigned to an existing employee or a new one is created if necessary.
- Employees receive their user accounts automatically through user account resources.

Basic Mechanisms for Employee and User Account Administration

The requirements on the company's user administration are often not only different in the existing target systems, but also in the individual areas of a target system. Even within an defined area of a target system there may be different rules for different user groups. For example, different rules for allocating user accounts can apply in the individual domains within a Active Directory environment.

A requirement could look like, for example:

- In domain A, a user account should be automatically created for each internal employee. The information for the ADS container and the Home Server are based on the department and location of the employee. Each user account in the domain, which is marked as a mail account, automatically receives an Microsoft Exchange mailbox. An exception to this is the system services user account.
- In domain B the user accounts are administrated independently of the employee data. Microsoft Exchange mailboxes can only be allocated by requesting them in the IT shop.

In order to fulfill the individual requirements of user administration, users can be divided into categories:

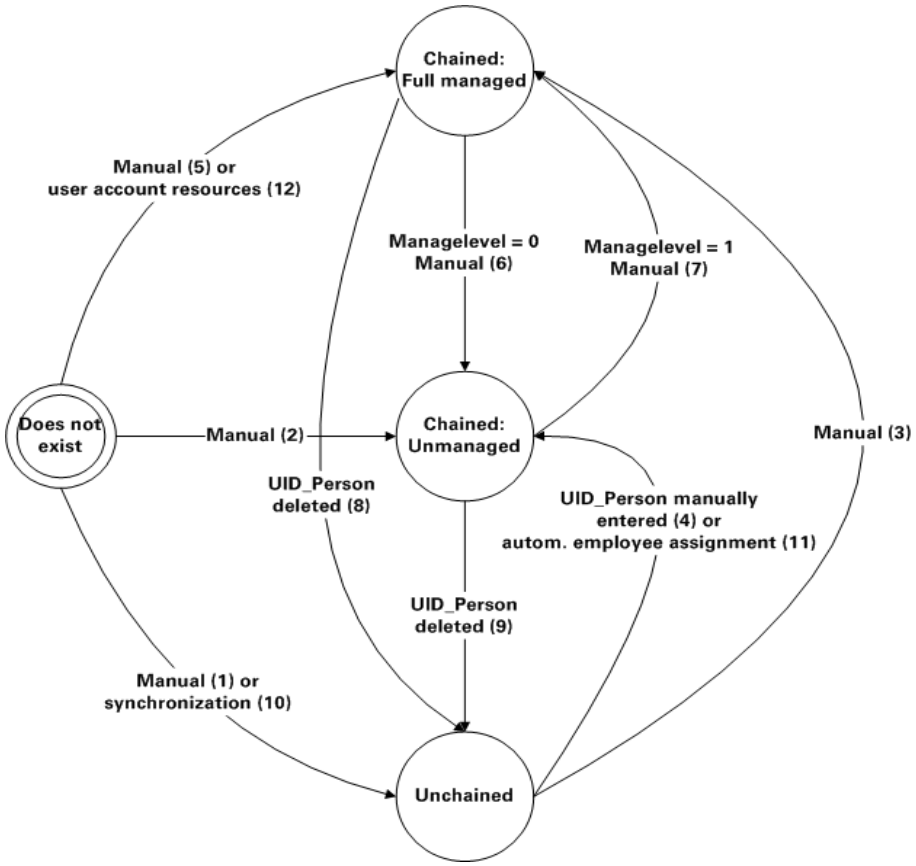
- Unlinked
  The user accounts are not linked to an employee and, therefore, do not inherit properties from that employee.
- Linked
  The user account is linked to an employee. The effect of the link can be specified by a freely definable manage level and therefore also defines the scope of the employee's inherited properites on the user accounts.

The Identity Manager supplies a configuration, for the "Linked" case, with the manage level:

- Unmanaged (ManageLevel = 0)
  The user accounts are assigned to employees, but do not inherit further properties from them.
- Full managed (ManageLevel = 1)
  The user accounts are assigned to employees and inherit their properties.

The following diagram should make the user account transitions clearer. It illustrates the default mechanisms integrated in the Identity Manager for employee and user accounts administration.

Transition States for a User Account



Manual Handling of User Accounts

In order to manage a user account independently from employee data, the user account is added manually and is not assigned to an employee. The user account is, therefore, not linked to an employee (UID_Person = " ") and has the state ”Unlinked“ (case 1).

If the user account is already linked to an employee through manual input (UID_Person<> " "), the user account manage level is set through internal processing and the user account changes its state to ”Linked:Unmanaged“. (case 2).

If a existing user account is manually assigned to an employee and at the same time the manage level is changed to Managelevel = 1, then the user account state changes from the state ”Unlinked“ to the state ”Linked:Full managed“ (case 3).

If a existing user account is manually assigned to an employee, the manage level is changed and the user account changes from the state ”Unlinked“ to the state ”Linked:Unmanaged“ (case 4).

If a existing user account is manually assigned to an employee and at the same time the manage level is adjusted (Managelevel = 1), the user account then has the state ”Linked:Full managed“ (case 5).

By changing the manage level an existing user account can change from the state ”Linked:Full managed“ to the state ”Linked:Unmanaged“. The manage level can only be changed for user accounts that are associated to an employee.

By deleting the employee entry in a user account that is associated to an employee (”Linked:Full managed“ or ”Linked:Unmanaged“), the user account always changes to the state ”Unlinked“ (cases 8 and 9).

Handling User Accounts during Synchronization

When a database is synchronized with a target system, the user accounts are always added without an associated employee and therefore, have an initial state of ”Unlinked“ (case 10). An employee can be assigned afterwards. This can be done manually over an automated employee assignment process using a process.

Assigning Employees Automatically to Existing User Accounts

Automated assignment of employees to existing user accounts takes place using comprehensive script and process processing. This mechanism can be carried out by adding a new user account with the state ”Unlinked“ (manually or with synchronization).

Automated employee assignment works in the modes:

- No (default behaviour)
  No automated assignment of employees to user accounts takes place.

- Search
  If no employee is assigned, then a suitable employee is searched for with defined conditions and the user account is assigned to that employee.

- Create
  If the user account is not assigned to an employee, a new employee is added and assigned to it.

- SearchAndCreate
  If there is no employee assigned to the user account, a suitable employee according to the defined conditions, is searched for and that employee is assigned the user account. If an employee cannot be found, a new employee is created and assigned to the account.

The modes ”Search“, ”Create“ and ”SearchAndCreate“ result in an employee being assigned to a user account. The user account then has the state ”Linked:Unmanaged“ (case 11).

This mode is set in a target system specific configuration parameter and has, therefore, a global effect on the target system. In order for the automated employee assignment to be used in different ways in the separate areas of a target system, the scripts and processes needs to be customized respectively. The criteria for automatically assigning an employee to a user account is also defined on a company specific basis. Please read the section Automatic Assignment of Employees to User Accounts on page 40 for more a more detailed description of automatic employee assignment.

Handling User Accounts with User Account Resources

The Identity Manager has special resources for automatically allocating user accounts to employees during working hours. These user account resources can be created for the respective area of a target

system, for example, for the different ADS domains of a Active Directory environment. If an employee does not yet have a user account in this area of the target system, a new one is created by assigning a user account resource to an employee using the integrated inheritance mechanism and subsequently processing a process. The manage level is set (Managelevel = 1) and the user account has the state ”Linked:Full managed“ (case 12).

There is one process per target system included in the default installation of the Identity Manager, which creates user accounts using user account resources. These can be used as templates for a company specific implementation of this method. How user account resources function is explained in detail in the section Creating User Accounts with User Account Resources on page 37.

Employee and User Account Administration

The requirements on the user administration in a company are often not only different in the existing target system, but also in the employee areas of a target system.

In an extreme case the requirements on the administration of the user accounts could appear as follows:

Target System Active Directory with Microsoft Exchange

- A user account should be created for every internal employee in domain A.
  The information for the ADS container and home server are based on the department and the location of the person. Every user account in the domain that is marked as mail account, is automatically assigned a Microsoft Exchange mailbox.

- In domain B the user accounts are handled independently from the personal data.
  Microsoft Exchange mailboxes can only be allocated through by request process.

Target System Lotus Notes

- All members of the sales department are automatically allocated a Lotus Notes mailbox.
  The members of the other departments can request a Lotus Notes Mailbox. The attributes of the postbox are determined independently of member’s department.

Target System SAP R/3

- All members of the personnel department are automatically allocated a user account in an SAP Client 101.

- The members of the ”purchasing“ department are automatically allocated a user account in the SAP Client 102 the moment they are assigned their appropriate role.

- The user accounts for the Client 103 are allocated exclusively through a request process.

Identity Manager uses different mechanisms to assign user accounts to employees.

Initial Assignment of User Accounts

The user accounts are initially read into Identity Manager from a target system via synchronization. In doing so, the existing employees can automatically be assigned to the user accounts. New employees can be created and assigned to user accounts if necessary. The criteria for these automatic assignments are defined on a company specific basis.
The automated administration level and with it the extent of the attributes an employee inherits on his or her account can be changed after checking the user accounts.The loss of user accounts through system changes can therefore be avoided. User account checking can be carried out manually or in by using scripts.

Assigning User Accounts during Work Hours

Identity Manager defines resources in order to allocate user account to employees during business hours. These user account resources can be created for each area of the appointed target system, for example the different domains of an Active Directory environment or the individual SAP clients of an SAP R/3-system. A priority is applied to the user account resources in order to be sure that a Microsoft Exchange mailbox, for instance, is only created when a user account is available.

An indvidual can obtain a user account via the integrated inheritance mechanism through direct assignment of user account resources to an employee or through assignment of user account resources to departments, cost centers, location or business roles. All company employees can be allocated special user account resources independent of their affiliation to the departments, cost centers, location or business roles. In Identity Manager it is possible to assign user accounts to articles that can be requested from the IT Shop. Then the department manager can request user accounts for his staff via the IT Shop.

Treatment of User Accounts and Personal Data during Deactivation

The handling of personal data, particularly during long-term or temporary absence of an employee, is dealt with differently in each company. There are companies which never delete personal data, but just deactivate it when the person leaves the company. Other companies want to delete the personal data but only after they are sure that all the user accounts have been deleted.

Since the topic of user administration is quite complicated, it is described in detail in a separate chapter Employees and User Accounts on page 25.

Handling Employees and User Accounts

At this point, we shall discuss the effects that the basic employee information has on the employee's user accounts. Certain employee master data is passed down to the employee's user accounts via templates. The template that are supplied can be customized to suit your requirements. The extent of the inheritence depends on the user account manage level. The Identity Manager supplies an initial configuration for mapping employee master data to user accounts with the manage levels:

- Unmanaged
  The user accounts are assigned to an employee but do not however, inherit other properties from the employee.

- Full managed
  The user accounts are assigned to an employee and inherit the employee's properties.

When user accounts are created with the manage level "Full Managed", the necessary data for the user accounts is composed by rules defined from the employee's master data. Creating user accounts is controlled by the following employee properties:

- Central user account

- Default email address

- Company data (department,location, cost center)

Central User Account

Configuration Parameter for Forming the Central USer Accounts

CONFIGURATION PARAMETER	MEANING
QER\Person\CentralAccount-GlobalUnique	If this configuration parameter is not set (default) the central user account for an employee is formed uniquely in relation to the central user accounts of all employees and the user account names of all permitted target systems. If the configuration parameter is not set, it is only formed uniquely related to the central user accounts of all employees.

The employee's central user account is used to form the user account login name in the active system. In the Identity Manager default installation, the central user account is made up of the first and the last name of the employee. If only one of these is known, then it that is used for the central user account. The Identity Manager check in any case, if a central user account with that value already exists. If this is the case an incremental number is added to the end of the value.

Example for the Forming of Central User Accounts

FIRST NAME	LAST NAME	CENTRAL USER ACCOUNTS
Mary		MARY
	Harlow	HARLOW
Mary	Harlow	MARYH
Mary	Harris	MARYH1

Default Email Address

The employee's default email address is displayed on the mailboxes in the activated target system. The default installation from the Identity Manager builds the default email address from the employee's central user account and the default mail domain of the active target system.

The default mail domain is determined by a script which includes the following configuration parameters in the given order.

Configuration Parameter Default Mail Domain

CONFIGURATION PARAMETER	MEANING
TargetSystem\Notes\DefaultMailDomain	Name of the default mail domain in target system Lotus Notes.
TargetSystem\ADS\Exchange2000\DefaultMailDomain	Name of the default mail domain in target system Microsoft Exchange.

The Identity Manager assumes that only one email system is used company wide. Usually the only one of the given configuration parameters is required to determine the active default mail domain and to set the required value. If this assumption is not correct and more that one email systems are in use, the script to determine the default mail domain has to be changed.

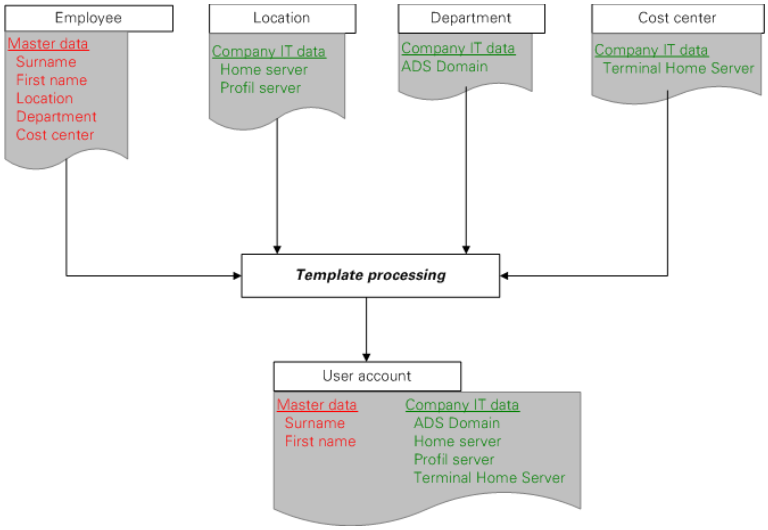
Determining the IT Operating Data for an Employee's User Account

An employee can only be assigned one primary location, one primary department, one primary cost center and one primary business role. The necessary IT operating data is ascertained depending on these assignments.

In order for an employee to create user accounts with the manage level "Full managed", the necessary IT operating data, for example, domain structure, home structure and profile server has to be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers and business roles (see also Setting Up IT Operating Data on page 99). The IT operating data is determined depending on the company structure and has to be correspondingly changed.

The process sequence for automatically assigning IT operating data to the employee's user account within the Identity Manager should be made clearer with the help of the following diagram.

Displaying IT Operating Data on top of a User Account



The data for the user accounts in the respective target system result from the basic employee data. The assignment of the IT operating data to the employee's user account is controlled over the primary assignment of the employee to a location, a department, a cost center or a business role (template processing).

For the operating systems SAP R/3 and SharePoint, the IT operating data is not found through an employee's assignment to company structures. The information required for creating user accounts for this target system are stored directly with the user account resource.

There are predefined templates included in the default installation for determining IT operating data that can be customized. The IT operating data necessary for automatically creating or changing employee user accounts and mailboxes in the target system, is itemized in the following table.

Target System Dependent IT Operating Data

TARGET SYSTEM	IT OPERATING DATA
Unified Namespace	Container (per proxy ID)

Target System Dependent IT Operating Data

TARGET SYSTEM	IT OPERATING DATA
LDAP	LDAP Container
Lotus Notes	Notes Server
	Notes certificate
	Mailbox template
Microsoft Exchange	mailbox storage
Active Directory	AD Container
	AD Home Server
	AD Profile Server
	AD Terminal Home Server
	AD Terminal Profile Server

Determining IT Operating Data

In order to make it possible to define IT operating data from departments, cost centers, locations and business roles, the configuration parameters need to cutomized. If no IT operating data results from assigning the employee to these structures, the default values for IT operating data are used. These default values are specified by configuration parameters.

If the configuration parameters are not set, the assignment of IT operating data to a user acount has to be done manually. To set up a user account automatically using user account resources it is absolutely necessary to set the configuration parameters!

The formatting rules for determining the IT operating data are newly calculated when a change is made to a configuration parameter. In certain circumstances this can result in a large number of objects being changed and saved and processes may be generated.

Activating IT Operating Data Assignments

The IT operating data can only be determined for automatic creation of user accounts or employee mailboxes in the target system using departments, cost centers and locations or defined default values when the following configuration parameters are set,.

Configuration Parameters for Activating IT Operating Data

TARGET SYSTEM	IT OPERATING DATA	CONFIGURATION PARAMETER
Active Directory	AD Container	TargetSystem\ADS\ADSContainer
	AD Homeserver	TargetSystem\ADS\Homeserver
	AD Profilserver	TargetSystem\ADS\Profileserver
	AD Terminal Homeserver	TargetSystem\ADS\Terminal-Properties\TerminalServer_Homeserver
	AD Terminal Profilserver	TargetSystem\ADS\Terminal-Properties\TerminalServer_Profileserver
LDAP	LDAP Container	TargetSystem\LDAP\LDAPContainer
Lotus Notes	Notes certificate	TargetSystem\Notes\Certifier
	Notes server	TargetSystem\Notes\Server
	Mail template	TargetSystem\Notes\MailTemplate
Microsoft Exchange	Mailbox	TargetSystem\ADS\Exchange2000\Mail-boxStore
Unified Namespace	Container	TargetSystem\UNS\UNSContainer

Determining Departments, Cost Center, Locations and Business Roles

The IT operating data for user accounts or mailboxes in the target system is detemined through the given structures. The configuration parameters have the following values in each case:

Department	The IT operating data is determined from the employee’s primary department.
Locality	The IT operating data is determined from the employee’s primary location.
Profitcenter	The IT operating data is determined from the employee’s primary cost center.
Org	The IT operating data is determined from the employee’s primary business role.

Configuration Parameter to Specify the Department, Cost Center and Location

TAGET SYSTEM	IT OPERATING DATA	CONFIGURATION PARAMETER
Active Directory	AD Container	TargetSystem\ADS\ADSContainer\ITDataFrom
	AD Profile Server	TargetSystem\ADS\Profileserver\ITDataFrom
	AD Home Server	TargetSystem\ADS\Homeserver\ITDataFrom
	AD Terminal Home Server	TargetSystem\ADS\TerminalProperties\TerminalServer_Homeserver\ITDataFrom
	AD Terminal Profileserver	TargetSystem\ADS\TerminalProperties\TerminalServer_Profileserver\ITDataFrom
LDAP	LDAP Container	TargetSystem\LDAP\LDAPContainer\ITDataFrom
Unified Namespace	Container	TargetSystem\UNS\UNSContainer\ITDataFrom
Lotus Notes	Notes Certificate	TargetSystem\Notes\Certifier\ITDataFrom
	Notes Server	TargetSystem\Notes\Server\ITDataFrom
	Mail file template	TargetSystem\Notes\MailTemplate\ITDataFrom
Microsoft Exchange	Mailbox storage	TargetSystem\ADS\Exchange2000\MailboxStore\ITDataFrom

Specifying the IT Operating Data Default Values

In a hierarchical structure, all the levels are initially tested in order to determine the IT operating data. If no valid IT operating data is found in this way, the previously stored defaults are used:.

Configuration Parameter for IT Operating Data Default Values

TARGET SYSTEM	IT OPERATING DATA	CONFIGURATION PARAMETER
Active Directory	AD Container	TargetSystem\ADS\ADSContainer\Default
	AD Home Server	TargetSystem\ADS\Homeserver\Default
	AD Profileserver	TargetSystem\ADS\Profileserver\Default
	AD Terminal Home Server	TargetSystem\ADS\TerminalProperties\TerminalServer_Homeserver\Default
	AD Terminal Profileserver	TargetSystem\ADS\TerminalProperties\TerminalServer_Profileserver\Default
LDAP	LDAP Container	TargetSystem\LDAP\LDAPContainer\Default

Configuration Parameter for IT Operating Data Default Values

TARGET SYSTEM	IT OPERATING DATA	CONFIGURATION PARAMETER
Lotus Notes	Notes Certificate	TargetSystem\Notes\Certifier\Default
	Notes Server	TargetSystem\Notes\Server\Default
	Mail file template	TargetSystem\Notes\MailTemplate\Default
Microsoft Exchange	Mailbox storage	TargetSystem\ADS\Exchange2000\Mail-boxStore\Default
Unified Namespace	Container	TargetSystem\UNS\UNSContainer\Default

Testing Default Values

When these parameters are set, a test takes place to see if the default values from the configuration parameters can be used to specify the IT operating data (fall-back solution). If this is the case, an email is send to a specified mailbox.

Configuration Parameters to Test the Defautl Values

TARGET SYSTEM	IT OPERATING DATA	CONFIGURATION PARAMETER
Active Directory	AD Container	TargetSystem\ADS\ADSContainer\Check-DefaultUsed
	AD Home Server	TargetSystem\ADS\Homeserver\Check-DefaultUsed
	AD Profileserver	TargetSystem\ADS\Profileserver\Check-DefaultUsed
	AD Terminal Home Server	TargetSystem\ADS\Terminal-Properties\TerminalServer_Homeserver\Check-DefaultUsed
	AD Terminal Profileserver	TargetSystem\ADS\Terminal-Properties\TerminalServer_Profileserver\Check-DefaultUsed
LDAP	LDAP Container	TargetSystem\LDAP\LDAPContainer\Check-DefaultUsed
Lotus Notes	Notes Certificate	TargetSystem\Notes\Certifier\CheckDefaultUsed
	Notes Server	TargetSystem\Notes\Server\CheckDefaultUsed
	Mail file template	TargetSystem\Notes\MailTemplate\CheckDefaul-tUsed
Microsoft Exchange	Mailbox storage	TargetSystem\ADS\Exchange2000\Mailbox-Store\CheckDefaultUsed
Unified Namespace	Container	TargetSystem\UNS\UNSContainer\Check-DefaultUsed

The default incoming email address in the respective target system, the default outgoing email address, the default language and the SMTP server need to be specified in the following configuration parameters.

Configuration Parameters for Mail Notification

CONFIGURATION PARAMETER	MEANING
Common\MailNotification	Notification input.
Common\MailNotification\DefaultAddress	Default incoming email address (To).
Common\MailNotification\DefaultCulture	Default language culture that emails are sent in if no language culture can be determined for a recipient.
Common\MailNotification\DefaultLanguage	Default language for send messages.
Common\MailNotification\DefaultSender	Default outgoing email address (From)
Common\MailNotification\SMTPPort	SMTP service port on the SMTP server (default : 25).
Common\MailNotification\SMTPRelay	SMTP Server dor sending messages.
TargetSystem\ADS\DefaultAddress	Default incoming email adress for notifying over actions in the target system Active Directory.
TargetSystem\ADS\Exchange2000\DefaultAddress	Default incoming email adress for notifying over actions in the target system Exchange 2000.
TargetSystem\LDAP\DefaultAddress	Default incoming email adress for notifying over actions in the target system LDAP.
TargetSystem\Notes\DefaultAddress	Default incoming email adress for notifying over actions in the target system Lotus Notes.
TargetSystem\SAPR3\DefaultAddress	Default email address (recipient) for messages about actions in the target system SAP R/3.
TargetSystem\SharePoint\DefaultAddress	Default email address (recipient) for messages about actions in the target system SharePoint.

Creating User Accounts with User Account Resources

You can define special resources in the Identity Manager to automatically allocate user accounts during working hours. These user account resources can be created by you for any area of the target system, e.g. for the different domains in a Active Directory Service environment. The procedure for setting up user account resources is described in the respective chapter for the target system.

A user accounts are created for employees through integrated inheritence mechanisms and subsequent processing by assigning user account resources to employees or company structures (departments, cost centers, locations, roles). Special user account resources can be automatically assigned to all the employees in a company, independent of their affiliation to departments, cost centers, locations or roles. It is also possible to assign user account resources to articles which can be requested from the IT Shop. A department manager can make requests from IT Shop for his staff.

If employees obtain their accounts via user account resources, they have to have a central user account and have to obtain their IT operating data over the assignment of a primary department, primary location or a primary cost center. The target system SAP R/3 and SharePoint are excluded here. In these

cases, the necessary information for creating user accounts is determined directly from the user account resource. The default email address is still needed to create a mailbox using user account resources. Read more in section Determining the IT Operating Data for an Employee's User Account on page 32.

Every user account resource has different manage levels for creating user accounts. A user account manage level is the deciding factor in the number of properties a user account inherits from an employee. See section Basic Mechanisms for Employee and User Account Administration on page 26 for more information.

A default manage level is defined for every user account resource. This manage level is used to determined the valid IT operating data when a user account is created. In the Identity Manager default installation, the processes are checked at the start to see if the employee aleady has a user account in the area of the target system that has user account resources. If there is no user account, a new one is created with the default manage level. If a user account already exists and is deactivated, then it is unlocked. In this case, you need to change the manage level of the user account afterwards.

Using Several User Account Resources within a Target System

If there are several areas within a target system to be administrated through user account resources, you have to create a separate user account resource for each target system area. The default installation expects a different default manage level for each user account resource. This allows an employee can have user accounts in different Active Directory domains, for example. An employee may be allowed by the Identity Manager to use several user account resources with the same manage level if it can be guaranteed that the user only has a user account in one target system area of the target system.

The target systems SAP R/3 and SharePoint are excluded. In this case, several user account resources with the same default manage level are allowed by default.

This behavior can be controlled by configuration parameters for each target system.

User Accounts Resource Configuration Parameter

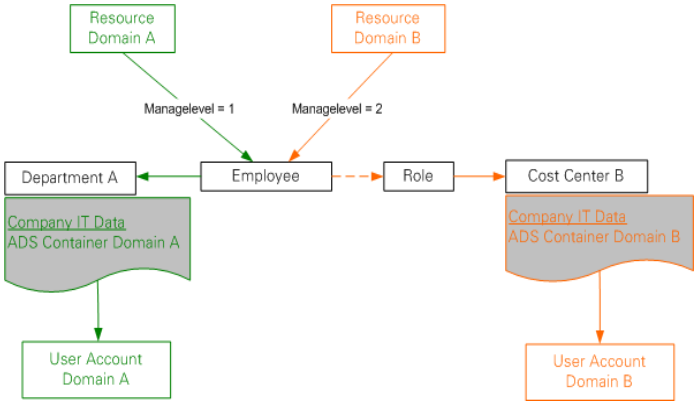
CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\Exchange2000\UniqueDefaultManageLevel	When the parameter is set, a different default manage level is expected for each user account resource in the target system (default). If the parameter is not set, each user account resource in the target system may have the same default manage level.
TargetSystem\ADS\UniqueDefaultManageLevel	
TargetSystem\LDAP\UniqueDefaultManageLevel	
TargetSystem\Notes\UniqueDefaultManageLevel	
TargetSystem\UNS\UniqueDefaultManageLevel	

Example 1:

There are two Active Directory domains in an Active Directory environment. The employees can have a user account in both of the Active Directory domains. The user account in domain A is allocated the company data via the employee's department. The user account in domain B is allocated the IT operating data via the employee's primary business role cost center.

Create a user account resource A for domain A and a user account resource B for domain B. In the user account resource A, set the default level to ”Full Managed (1)“. The manage level ”Full Managed (1)“ uses the Identity Manager default templates to determine the IT operating data. Set the default level to ”Full Managed (2)“ in the user account resource B. In the case of ”Full Managed (2)“, you need to extend the templates so that the IT operating data can be determined via the employee’s primary business role cost center.

Creating User Accounts using User Account Resources (Example 1)



When the employee is assigned the user account resources, subsequent script and process handling ensure that the employee obtains the user accounts in both domains.

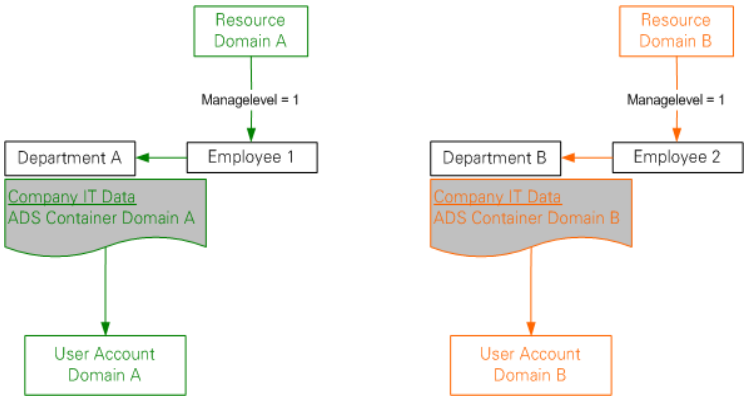
Example 2:

There are two Active Directory domains in an Active Directory environment. The employees can only have a user account in one of the Active Directory domains. The department operational data is used to decided whether the user account is created in domain A or domain B.

Create a user account resource A for domain A and a user account resource B for domain B. Set the manage level to ”Full Managed (1)“ in both resources. This manage level uses the Identity Manager default templates to determine the IT operating data.

If the employee belongs to department A, he or she obtains (by dynamic assignment, for example) the user account resource A and the resulting user account is in domain A. If the employee belongs to department B, he or she is issued the user account resource B and a user account in domain B.

Creating User Accounts using User Account Resources (example 2)



Templates and Processes for Implementing User Account Resources

The Identity Manager supplies a configuration the manager level ”unmanaged“ and for the manage level ”Full managed” for using with user account resources. These manage levels are taken into account in the supplied templates. You can define more rule levels for mapping manage levels depending on your requirements. In this case, you need to extend the templates with the procedure for additional manage levels.

There is one process respectively pro target system contained in the Identity Manager’s default installation for setting up user accounts using user account resources. These can be used as templates for the company specific implementation of the method. You can find these under the event ”Insert“ by object ”PersonHasRessourceTotal“. See chapter Handling Processes in Identity Manager for more detailed information about the Identity Manager processes.

The name of the process is put together as follows:

```
VI_PersonHasRessourceTotal_Autocreate_<Benutzerkontentabelle>
where:
<AccountTable> = Table that contains the user accounts;
for example:
ADSAccount (Active Directory user),
ADSAccountMailObject(Microsoft Exchange - recipient)*,
LDAPAccount (LDAP),
NotesUser (Lotus Notes user),
SAPUser (SAP user account),
SPSUser (SharePoint user account)
UNSAccount (Unified Namespace user account)

*) Mapping of Exchange relevant information in the table ”ADSAccount“
```

Automatic Assignment of Employees to User Accounts

When employees are automatically assigned, the employee master data is created based on the existing user accounts. This mechanism can take place after a new user account has been set up by manual entry or by synchronization. However, this procedure is not part of the standard the Identity Manager procedure.

The procedure can be put into action in order to create employee data sets from the existing user accounts in a target system during synchronization. Synchronization initially loads the user accounts from the target system into the Identity Manager. Automatic assignment of employees to already existing user accounts can take place by subsequently changing scripts and processes. If necessary, new employees can be created and user accounts assigned to them. The procedure can also be used during normal working hours. When a user account is set up, an employee is searched for by deferred script and process processing and then assigned. A new employee can be created if necessary depending on the configuration.

If you set off this procedure during working hours, automatic assignment of employees to newly created user accounts takes place from that moment on. This method does not affect user accounts which existed before this point in time. If you deactivate the procedure again later, then the changes that follow also only affect newly created user accounts. Already existing employee assignments to user account remain intact.

The criterian for automatically assigning employees to user accounts can be customized to meet the company’s needs.Read more in section Mapping Properties during Automatic Employee Assignment on page 42.

Configuring Automatic Employee Assignment

In the Identity Manager default installation, the automatic assignment of employees to user accounts is controlled by the configuration parameters shown below and is globally effective. A distinction is made here between the synchronization and the default methods.

Configuration Parameter for Automatic Employee Assignment

TARGET SYSTEM	CONFIGURATION PARAMETER
Active Directory	TargetSystem\ADS\PersonAutoDefault
	TargetSystem\ADS\PersonAutoFullsync
LDAP	TargetSystem\LDAP\PersonAutoDefault
	TargetSystem\LDAP\PersonAutoFullSync
Lotus Notes	TargetSystem\Notes\PersonAutoDefault
	TargetSystem\Notes\PersonAutoFullsync
SAP R/3	TargetSystem\SAPR3\PersonAutoDefault
	TargetSystem\SAPR3\PersonAutoFullsync
SharePoint	TargetSystem\SharePoint\PersonAutoDefault
	TargetSystem\SharePoint\PersonAutoFullSync

Each configuration parameter has one of the permitted modes:

- NO
  No automatic assignment of employees to user accounts takes place. This is the default value, that is also displayed when the configuration parameter is not active.

- SEARCH
  If an employee is not assigned, the matching employee is searched for based on defined conditions and the employee found is assigned to the user accounts. If an employee is not found, no new employee is added.

- CREATE
  If the user account is not assigned to an employee, a new employee is always added, some of the properties initialized and the employee is assigned to the user account.

- SEARCH AND CREATE
  If the user account does not have an employee assigned to it, a matching employee is searched for based on defined conditions and the employee that is found is assigned to the user account. If no employee is found, a new one is added, some of the properties are initialized and the employee is assigned to the user account.

If a user account is linked to an employee because of the current mode, the user account is given the manage level ”Unmanaged“ through an internal process. You can change this manage level later.

The configuration parameters are evaluated in the Identity Manager default installation insert and update processes that are target system dependent and thus determine the execution mode. The name s of the corresponding processes are ”Search and Create Person for Account“ and ”Search and Create Person for Account (Fullsync)“ .

Processe steps can be used as templates in order to be put into effect the automatic employee assignment in different areas of a target system, for example, the separate domains of a Active Directory environment.

Mapping Properties during Automatic Employee Assignment

You can specify the criterian for automatic assignment of a user account to an employee to suit company requirements. Specifying the search conditions for the assignment of an employee to a user account and the properties with which the employee is initalized, is done by scripts. The name of the script is:

```
VI_PersonAuto_<targetsystem>
where:
<targetsystem> = short name of the targetsystem concerned;
for example ADS, LDAP, Notes, SAP, SharePoint
```

These scripts are implemented for each target system in the Identity Manager default installation and can be used as templates to be customized to fit the company's needs. In the default installation automatic assignment of the employee takes place based on the central user account. In order to avoid adding employees to used system user acounts and service accounts, you need to define an exclusion list in the scripts that can be changed to accomodate company specific features if necessary.

When automatic employee assignment is carried out in the "CREATE" mode, some of the properties of the user account are passed on to the new employee object. Initializing the employee properties takes places using the respective script "VI_PersonAuto_<targetsystem>". Initializing the properties when an employee is being created for a user account can take place through the evaluation of the entry in the table "Dialognotification". In this table the connected properties are mapped as a bidirectional pair through the formatting rules. The evaluation of the entries in "Dialognotification" are exemplified in the initialization of an employee's surname as shown below.

Example:

The last name of an Active Directory user account is made up from the surname of the employee.

Value template for "ADSAccount.Surname":

```
Value = $FK(UID_Person).Lastname$
```

If the employee's surname changes the last name of the ADS user changes too. The column "Person.Lastname" is therefore the sender and the column "ADSAccount.Surname" is the receiver.

Relationship as in the table "Dialognotification":

```
Person.Lastname --> ADSAccount.Surname
```

The table "Dialognotification" can be used to help with the initialization of the properties for a new employee in that the relationships can be removed in reverse. The surname of an employee can be replaced with the surname of the ADS user. Thus, certain presets for the employee object can be automatically generated. However, only explicit relationships can be removed.

Example:

The display name of an Acitve Directory user account should be made up of the surname and the firstname of an employee.

Relationship according to the table "Dialognotification":

```
Person.Lastname --> ADSAccount.Displayname
Person.Firstname --> ADSAccount.Displayname
```

The "Person.Firstname" and "Person.Lastname" cannot be determined form the "ADSAccount.Displayname", since this is a compound value.

In order to make mapping of employee properties to user account properties easier, the script "VI_PersonAuto_GetPropMappings" can be used. This script evaluates the relationship of the properties

as used in the table ”Dialognotification“. The script creates a VB.Net script code and the possible assignments, when it is run by the ScripDebugger. This code can subsequently be inserted into the respective script ”VI_PersonAuto_<targetsystem>.

Example Version of a ”VI_PersonAuto_GetPropMappings“ Script

```
' PROPERTY MAPPINGS from ADSAccount to employee

' ADSAccount.Initials --> Person.Initials
' ADSAccount.Mail --> Person.DefaultEmailAddress
' ADSAccount.Department -->Person.UID_Department


Try
Person("Initials").NewValue = Acc.GetValue("Initials").String
Catch ex As Exception
End Try

Try
Person("DefaultEmailAddress").NewValue = Acc.GetValue("Mail").String
Catch ex As Exception
End Try

Try
Person("UID_Department").NewValue = Acc.GetValue("Department").String
Catch ex As Exception
End Try
```

Changing Employee Master Data

In the following sections, we only examine the master data that affects the user account of an employee with the manage level ”Full managed“ when it is changed in the Identity Manager default installation.

General Changes

This process concerns all changes to data relating to an employee’s telephone number, fax number, mobile telephone, street, postal or zip code and changes the data in the target system users that are assigned to the employee in so far as this data is represented in the respective target systems.

Changing an Employee’s Name

Changes to employee’s names influences how an employee’s central user account is set up. The central user account is made up of, according to the formatting rules, the first and last names and used as template for all relevant user accounts. When a user account is added, other formatting rules control how the home and profile directories are set up from the central user account that also require customizing when changes are made.

Employee Job Rotation Inhouse

Job rotation is affected by changes to the company data location and department. With this, the company operations are automated in the Identity Manager, with respect to the administrative tasks for alterations to the target system dependent IT operating data. There are other sub-processes for each target system because of the system dependent differences in the target systems regarding the actions necessary for changing departments.

Handling Disabling and Deletion of Employees and User Accounts

How employees are handled, particularly in the case of permanent or partial withdrawal of an employee, varies between individual companies. There are companies that never delete employees, only deactivate them when they leave the company. Other firms wish to delete the employee, but first when they have ensured that all the user accounts are removed.

Temporary Deactivation of an Employee

Effect Configuration Parameter for Temporarily Deactivating an Employee

CONFIGURATION PARAMETER	MEANING
QER\Person\TemporaryDeactivation	When this parameter is set, the employee's user accounts are also temporarily deactivated.

The employee is currently not in the company, he or she is expected to return at a predefined date. The desired behaviour could be to disable the user account and remove all group memberships. Or the user accounts could be deleted and reestablished with the employee's return even if it is with a new system identification number (SID).

Temporary deactivation of an employee is controlled by:

- The configuration parameter "QER\Person\TemporaryDeactivation"
  If the configuration parameter is set, the employee's user accounts are also deactivated for the period of deactivation.
- The option <temporary deactivation>
- The end date for the deativation (<temporary deactivated until>)
  This is implemented by the scheduled task "Activate temporarily deactivated user accounts" that checks the final date and reactivates the employee and the associated user accounts when the date is reached.

Employee's user accounts that are aleady deactivated before a temporary deactivation of an employee. are also reactivate at the end of the period.

Permanent Deactivation of an Employee

The employee is permanently deactivated. All the employee's user accounts are deleted or deactivated or the group memberships are removed. The desired method has to implemented on a company specific basis. Permenant deactivation of an employee is started by:

- The option <Deactivated permanently>
  Manually setting the option <Deactivated permanently> ensures that the leaving date is set to the deactivation date and that all the employee's user accounts and mailboxes are disabled.
- Reaching the leaving date
  Deactivation can also be controlled by the leaving date. The specified leaving date is regulary checked by the scheduled task "Disable user accounts of former employees". When the leaving date is reached the option <Deactivated permanently> is set.

Deferred Deletion of an Employee

Configuration Parameter for Deleting an Employee

CONFIGURATION PARAMETER	MEANING
QER\Person\User\DeleteDelay	Delay the deletion of user accounts (-1= delete immediately, otherwise: delete when value is exceeded)

When an employee is deleted he or she is tested to see if user accounts are still assigned or not. The employee is marked to be deleted and with that, is barred from any further processing. Although deletion is already initiated, it has not yet taken place. After the user account is deleted, the employee is deleted. The deletion procedure can be rolled back within a define period of time. Depending on the setting of the deletion delay in the parameter ”QER\Person\User\DeleteDelay“ it is possible to roll back the procedure of deleting the user accounts and mailboxes of an employee in the context menu <Undo delete>. Once the defered deletion period has expired it is no longer possible to restore theuser accounts.

Disabling and Deleting through User Account Resources

If you are managing the user accounts with user account resources, you can define the method you want for handling the user accounts when disabling or deleting. You can define special handling for each area of a target system by using the connection between an area of a target system and a user account. Setting up user account resources is described in the respective chapter for the target system.

Inheriting Resources

Define the inheritance method for a each user account resource yourself. The inheritance options of previous resources are overwritten. You may want employees that are disabled or marked for deletion to inherit user account resources to ensure that all necessary permissions are made immediately available when the employee is reactivated at a later time. The following user account resource options are available for mapping inheritance behavior:

- Inherit resources if permanently disabled
- Inherit resources on deferred deletion (currently not in use)
- Inherit resources if temporarily disabled
- Inherit resources on security risk

If the allocated user account resource is not passed on when an employee is disabled then the employee‘s user account that resulted from this resource assignment is deleted.

If the user account resource is not passed on when the employee is disabled, the user account associated with the employee that was created by this resource assignment, is deleted.

Handling User Accounts

How user accounts are handled can be specified for the different manage levels by the user account resources. In order remove permissions from an employee when he or she is being deactivated or deleted, the employee’s user accounts can be disabled. If the employee is activated again at a later date, the user accounts can also be reactivated.

Handling Group Memberships

You can specify handling for group memberships for the different manage levels by the user account resources. If an employee is deactivated or marked to be deleted, a user account resource that prevents the inheritance of group memberships for the area of the target system. This method can be requested if the employee's user accounts and mailboxes are disabled and therefore is not a member of the distribution list. During the deactivation period, no inheritance procedures should be calculated for this employee. Existing group memberships are deleted. The following manage level options are available on user account resources for handling user accounts:

- Inherit groups if permanently disabled
- Inherit groups if deletion is deferred
- Inherit groups if temporarily disabled.
- Inherit groups on security risk
- Inherit groups if user account disabled

Entering Employee Master Data

Tools:
Identity Manager with application role <Employee>/<Administrators>
Manager

Effective Configuration Parameters

CONFIGURATION PARAMETER	MEANING WHEN SET
QER\Person	Preprocessor relevant configuration parameter to control the type components for employee administration. If the parameter is set, the employee administration components are available. Changing it the requires recompiling the database.

In the Identity Manager, you can manage master data for company employees as well as external employees. The term 'employee' will be used in the following to describe internal and external employees alike as the master data is the same for both.

Enter employee master data in the Manager in the category <Employees>. Employees are filters by different criterion in this category. Take care that you fill in all mandatory fields when you edit the master data. Certain master data is inherited by the employee user account through templates. The scope of inherited master data depends on the user account's manage level and can be customized.

Employee Master Data

Configuration Parameter for General Personal Master Data

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\ComplianceCheck\Calculate-RiskIndex	Preprocessor relevant configuration parameter controlling calculation of an employee's risk index. If the configuration parameter is enabled, the risk index is determined depending on the employee permssions. Changes to this parameter require compiling the database.

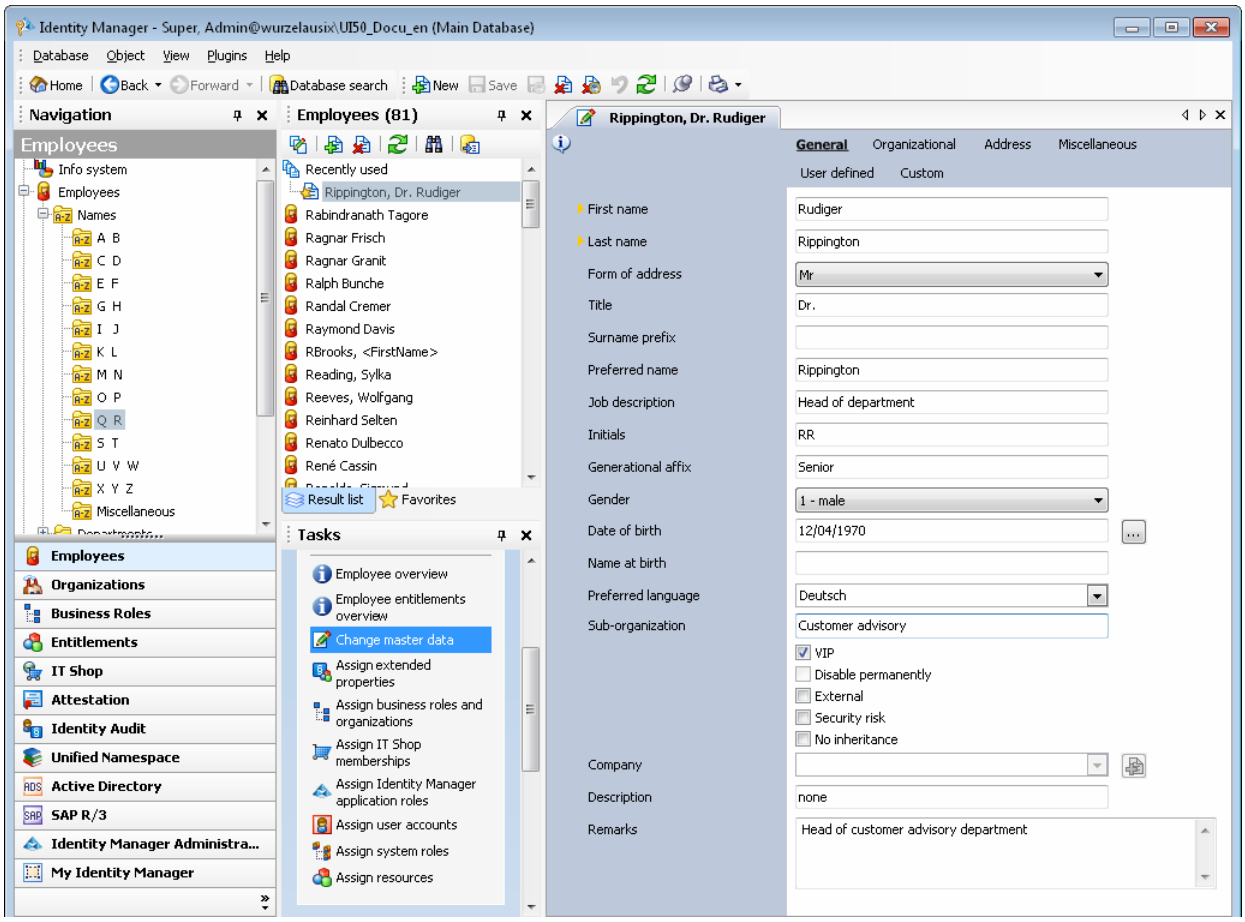
Enter the employee's general information such as name, surname, title, form of address, affix, job description, initials, surname prefix, generation label, date of birth, maiden name, sex. The input fields <Initials> and <Form of address> are preset with a value generated by formatting rule supplied as default by Quest Software. Other general features are labeling an Employee as VIP and entering sub-organizations.

Setting the option <Disable permanently> causes an employee to be permanently disabled. If you set this option manually then the last working day is the same as the day the account is disabled. As an alternative, you can manually set the permanent disable flag on the last day of work input field (see Organizational Employee Master Data on page 49). When the last working day is reached the <Disable permanently> option is automatically set. Read section Deferred Deletion of an Employee on page 45 for more information about this.

The option <External> differentiates between an internal and an external company employee. In the default version of the Identity Manager external employees are excluded from automatic user account resource assignment, for example. Enter a company for an external employee. Enter new companies

using the insert button next to the input field <Company> or under <Basic configuration data>\<Business partners>.

Employee Master Data - General



If the employee poses a security risk for the company at any time, set the option <Security risk>. This prevents employee of this type from inheriting resources and permissions when particular configurations arise and the user accounts are locked. For more information, read section Disabling and Deleting through User Account Resources on page 45.

Use the option <No inheritance> to control inheritance of company resources to employees. Employees inherit all the company resources of all company structures that they are assigned to. Enable this option to prevent inheritance of company resources through departments, cost centers, locations and business roles.

A risk index is calculated to evaluate the risk of an employee in the context of identity audit based on their permissions. An employee‘s risk index is determined from the risk indexes of their user accounts. The input field is only visible if the configuration parameter ”QER\ComplianceCheck\CalculateRiskIndex“ is set. For more information, read the section Risk Evaluation on page 427.

Enter additional information about an employee in the fields <Description> and <Remarks>.

Organizational Employee Master Data

Configurations Parameters for Setting up Employees

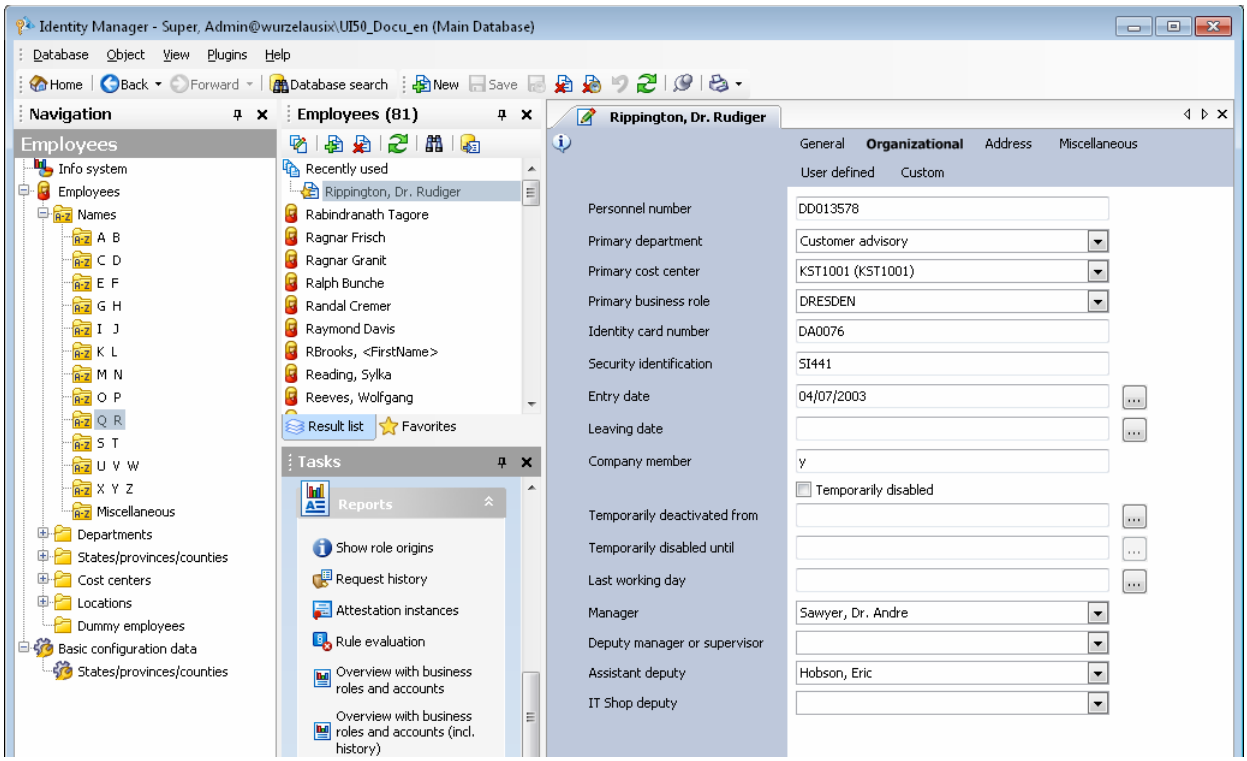
CONFIGURATION PARAMETER	EFFECT
QER\Person\AutoIncrementIdentityNumber	This parameter controls the allocation of the IdentityNumber to employees. If the configuration parameter is set, newly added employees are given an identity number that is 1 larger that the previous one, when the object is saved.
QER\ITShop	Preprocessor relevant configuration parameter for controlling the database model components for the IT Shop. If the parameter is set, IT Shop components are available. Changes to the parameter require recompiling the database.

Organizational input mainly concerns the personnel number, the security identification, the company membership, position of responsibility as well as the identity card number. The configuration parameter ”QER\Person\AutoIncrementIdentityNumber“ controls the allocation of identity card numbers to employees. If the configuration parameter is set, newly added employees are automatically given a unique identity card number, incremented by the value ”1“ from the previous card number, when the data is saved. If the configuration parameter is not active the identity card number has to be manually allocated.

You can specify which primary department and cost center the employee belongs to. You can also assign a primary business role. This data is used to determine the necessary IT operating data for the user accounts and mailboxes the employee uses (see section Determining the IT Operating Data for an Employee’s User Account on page 32). When the Identity Manager is configured accordingly, an emplo-

yee can receive company resources through this primary assignment (department, cost center, business role). Refer to section Assigning Company Resources through Roles on page 78.

Employee Master Data - Organizational



When a new employee is added the entry date is set to the current data.

Enter a leaving date so that the employee with its user accounts can be locked on a specific date. The leaving date is checked regularly by the scheduled task ”Lock user accounts from dismissed employees.“. When the date is reached, the option <Disable permanently> is set and with that, the employee is permanently locked.

If a leaving date is specified then it is transferred to the user account as the closing date for the account. Any existing closing date is overwritten. If the leaving date is deleted by the employee, the user account closing date remains intact!

In addition to the leaving date you need to enter the last working day for an employee. The last day of work is taken from the leaving date as default. Change the date of the last day of work when, for example, the employee leaves the company on a specified day but should still have access to the data for a while.

As well as disabling an employee entirely, the Identity Manager offers the possibility to disable an employee and its user account for a limited duration up until a specified date. Use the input fields <Temporarily deactivated from> and<Temporarily disabled until> to do this. A scheduled task ”Enable tem-

porarily disabled accounts‟ is implemented that intermittently monitors the end date and reenables the employee and its user accounts when the date is reached.

An employee‘s user accounts that were already disabled before the employee was temporarily disabled are also reenabled once the deactivation period is over.

For more information about how to handle employees and their user accounts, read the section Handling Disabling and Deletion of Employees and User Accounts on page 44

You can specify several managers and deputies for a employee. An employee’s manager is responsible for approving requests within the IT Shop in a defined approval process (assuming this functionality is enabled). If the employee is an approver in the IT Shop himself, you can enter an IT Shop deputy for example, for a vacation period. This IT Shop deputy is also authorized to make apporvals and can make requests on behalf of the employee. The input field is only visible if the configuration parameter ”QER\ITShop‟ is set. Read the section Selecting an Approver on page 59 for more information.

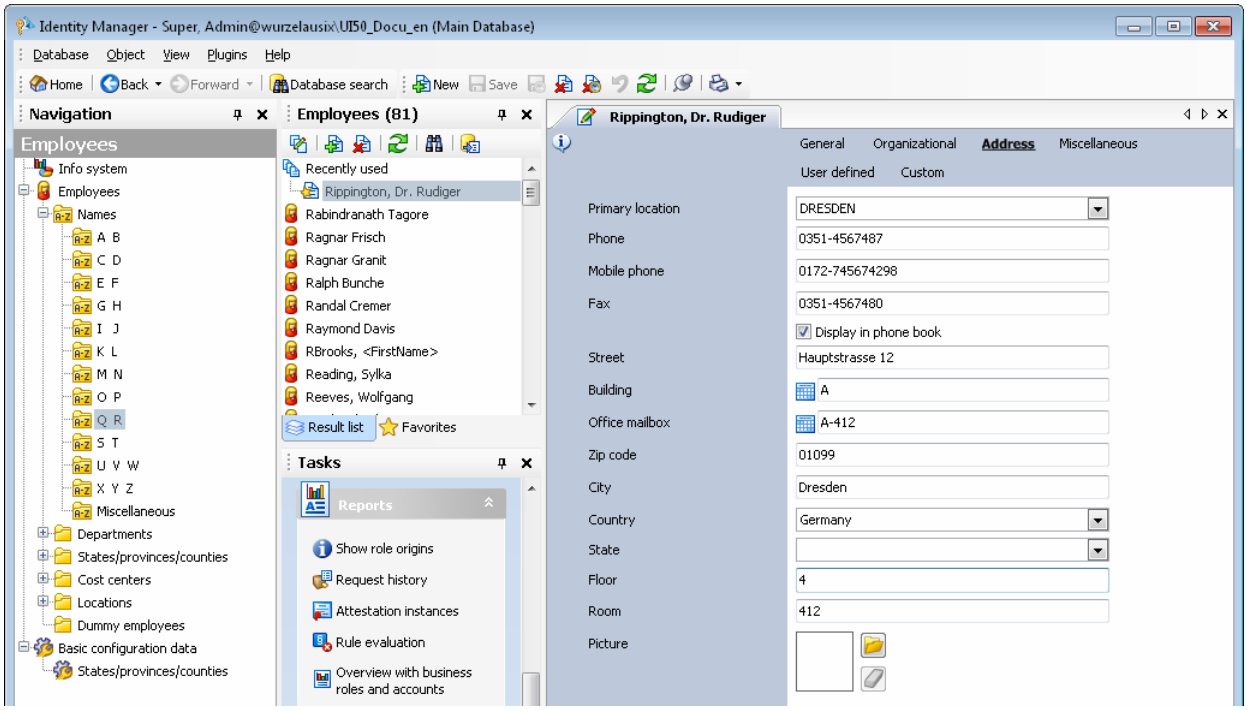
Address Data

You can specify which primary department the employee belongs to. This is used to determine the necessary IT operating data for the user accounts and mailboxes the employee uses. Read more in the section Determining the IT Operating Data for an Employee’s User Account on page 32. The assignment of a primary structure can also be made. An employee can receive company resources over this primary assignment when the Identity Manager is accordingly configured. Refer to section Assigning Company Resources through Roles on page 78.

Enter the employee’s address and telephone numbers. In addition, you can specify, if an employee should be automatically entered into the internal telephone directory or not (the internal telephone directory is not supplied by the Identity Manager). Furthermore, you can assign a state and a country to the employee. This information is accessed when determining, for example, the language for email notifications or the default hours for processing IT Shop workflows.

Enter the required states in the category <Basic Configuration Data>\<States or provinces>. You can import a picture of an employee into the database. To do this, use the button next to the <Picture> field to select the path where the picture can be found.

Employee Master Data - Address



Miscellaneous Employee Master Data

Configuration Parameters for Miscellaneous Employee Master Data

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Person\CentralPasswordHistoryLength	A password history is created. The value entered here corresponds to the explicit number of new passwords required before an old password can be reused. There is a test against the employee's main password.
QER\Person\MasterIdentity	Preprocessor relevant configuration parameter for controlling the component parts for administrating several identities for one employee. Changes to the parameter require recompiling the database. If the parameter is set, several logical employees can be handled in the database for one physical employee (for example, an employee has different identities and account characterists at different branches).
QER\Person\UseCentralPassword	The employee's main password is automatically mapped to the employee's user accounts in all permitted target systems.
QER\Person\UseCentralPassword\PermanentStore	This configuration parameter controls the storage period for central passwords. If the parameter is set, the employee's central password is permenantly stored. If the parameter is not set, the central password is only to publicize the target system and is subsequently deleted from the Identity Manager database.
TargetSystem\SAPR3	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the target system SAP R/3. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.

An employee's central user account affects the composition of user accounts in each target system. The employee's central user account is used to create user accounts names in each target system when user accounts are created automatically from user account resources. If you use the automatic method integrated into the Identity Manager to assign employees based on existing user accounts, then the employee is found and assigned with respect to on the central user account. These methods are explained in more detail in the sections Creating User Accounts with User Account Resources on page 37 and Automatic Assignment of Employees to User Accounts on page 40. The central user account is still used for logging onto the Identity Manager tools. See section Logging into Identity Manager Tools on page 125 for more details.

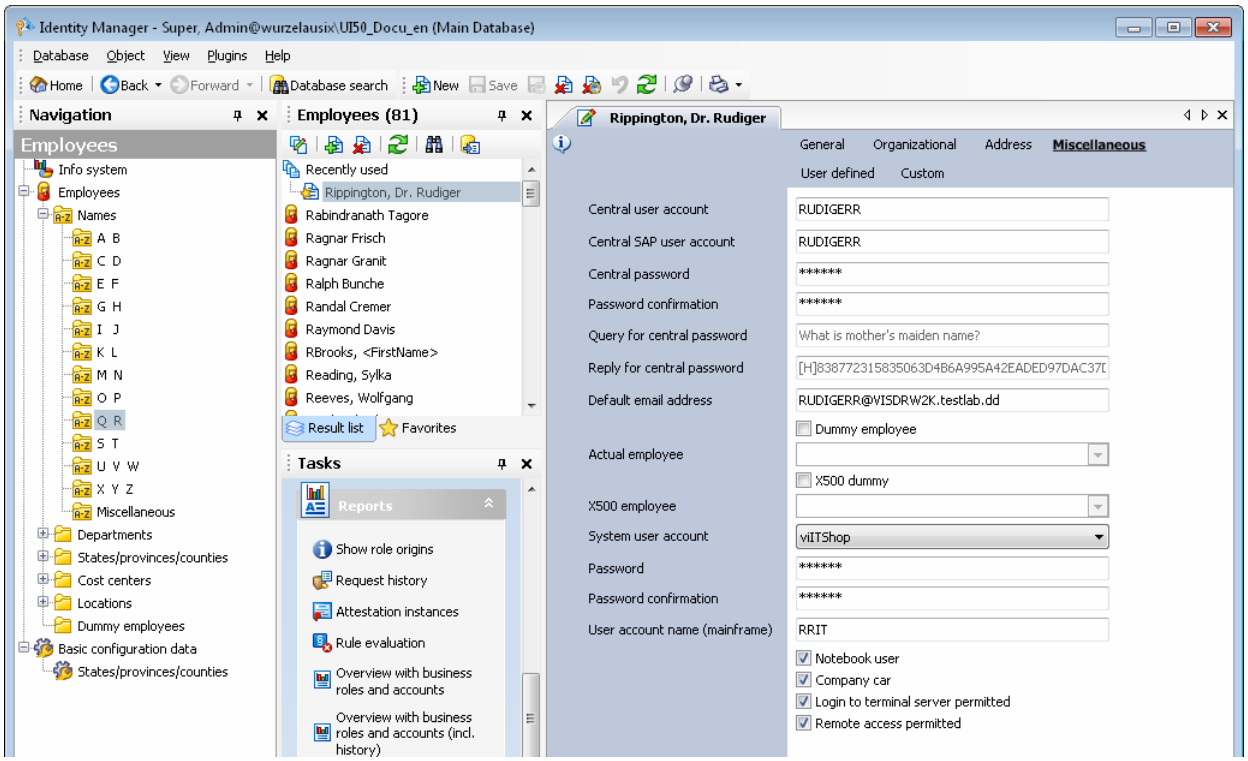
To define a central user account for an employee in the target system SAP R/3, use the input field <SAP central user account>. The input fields is only visible when the configuration parameter "TargetSystem\SAPR3" is set. Use the field <Central user account> for all other systems. The central user account is made up of the first and last names of the employee in the Identity Manager default version. Refer to the section Handling Employees and User Accounts on page 30 for more detailed information about the forming of user account names.

Enter a central password for the employee. Depending on the configuration parameter "QER\Person\UseCentralPassword", the central password is mapped to the user account of an employee in each of the target systems. Use the configuration parameter "QER\Person\UseCentralPassword\PermanentStore" to specify whether an employee's central password is permanently saved in the Identity Manager database or only until the password has been published in the target system. The configuration parameter "QER\Person\CentralPasswordHistoryLength" controls the password history. The given value corresponds to the number of unique new passwords that have to be used before an old one can be reused. The employee's central password is the one that is tested.

The input of a query and a reply for a central password plays a role when using the IT Shop. The query-reply combination is absolutely necessary for the password reset method that is used in this case.

The default email address is used to setup mail boxes for an employee in separate target systems. This data is absolutely necessary for autmatically creating mailboxes. In the default version of the Identity Manager, the default email address is composed of the employee's central user account and the default mail domain of the active target system. You can find more detailed information about the composition of the default email address and its effect on creating mailboxes in the section Handling Employees and User Accounts on page 30.

Employee Master Data - Miscellaneous



To set up a special case, the option <Dummy employee> is available to you. If an employee has several user accounts in a target system that should be assigned to different groups, then a separate "Dummy" employee should be set up for each user account. For each dummy employee a link can be set up to the "real" employee. If an employee has several X500 entries that differ in properties, you can also use a "Dummy" employee. Label the employee with the option <X500 dummy> in this case and configure a link to the real X500 employee.

Another special case is to differentiate employee data into main identity and subidentity. If an employee works with different identities for organizational reasons, you can bundle them by introducing a main identity. This allows permissions to be tested for each subidentity or for the main identity including all subidentities. Refer to section Mapping Multiple Employee Identities on page 58 for more.

Enter the system user with which the employee can log onto the Identity Manager administration tools. Enter a password for the system login in case several employees use the same system user, but each employee has their own password. The login data is examined by the authentication module in use (which may need to be enabled). For more information, refer to section Logging into Identity Manager Administration Tool as System User on page 129.

If the employee should have access to the mainframe with his or her user account, enter the required logon name in the field. The options <Notebook user> and <Company car> are only informative, The data <Remote access permitted> and <Login to terminal server permitted> are important for setting up user accounts with access permissions to a terminal server.

User Defined Employee Master Data

This tab for entering additional company specific information for an employee. The display names, formats and formatting rules for the input fields (default <Spare field no. 01-10>) can be customized to your requirements with Designer.

Additional Tasks for Managing Employees

After you have enter the employee's master data, you can apply various task to the person. You can see the most important information about an employee on the overview form. The tasks menu provides different forms with which you can peform the following tasks.

Add Employees to Company Structures

Tools:
Identity Manager with application role <Business roles>\<Administrators> or <Organizations>\<Administrators>
Identity Manager as manager or assistant deputy for the business role or organization
Manager

The default method for assigning company resources is through direct assignment. By doing this, employees are assigned to business roles, departments, cost centers and locations depending on their function in the company and they inherit company resources through these assignments.

You use the employee's master data form to make their primary assignments to a department, a location, a cost center or a business role. You can enter the employee into other company structures using the task <Assign business roles and organizations>. The employee can also inherit company resources via these secondary assignment if the configuration parameters are appropriately set. You can find further information in the section Assigning Company Resources through Roles on page 78. If the emnployee fulfils the requirement for dynamic roles, then they are dynamically add to the appropriate company structure. Refer to section Working with Dynamic Roles on page 100.

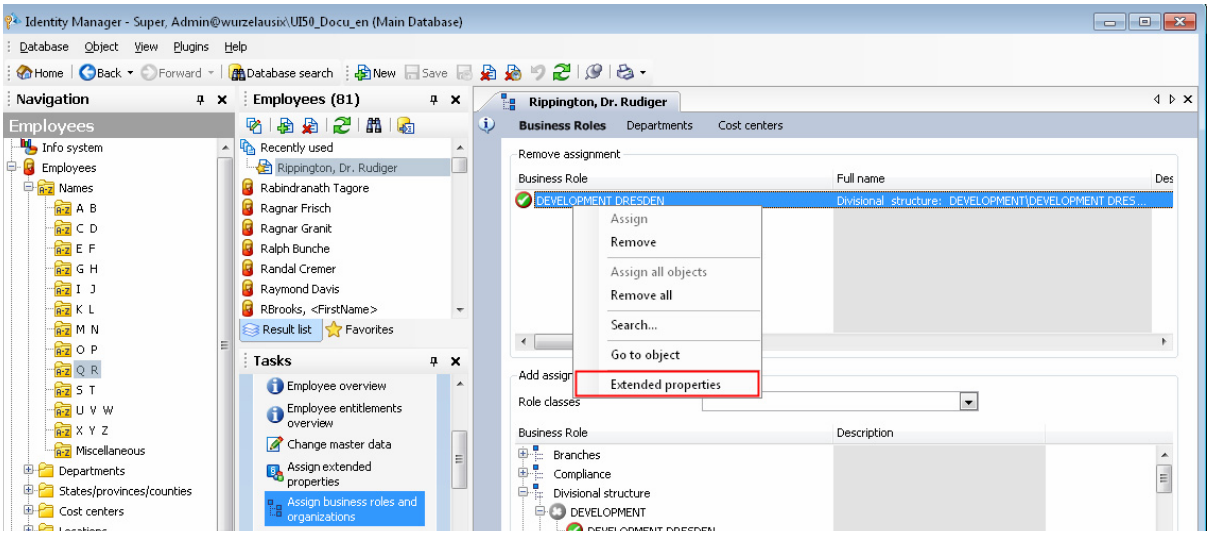
Specify Deputies in Company Structures

Tools:
Identity Manager as manager or assistant deputy for the business role or organization
Manager

After you have assigned a business role, a department, a cost center or a location, you can specify a deputy for the employee in each of the structures respectively. The assignment has to saved previously

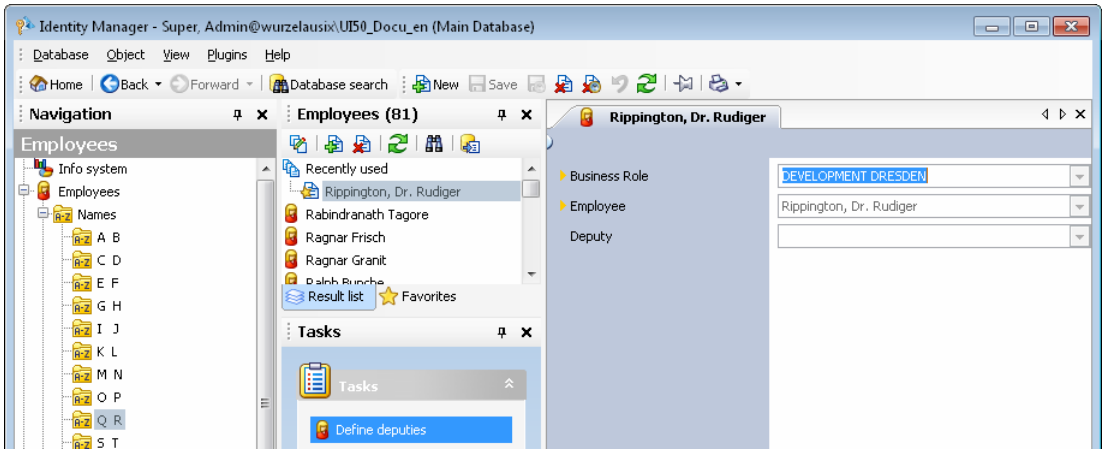
in order to do this. Select an entry on the form and use <Extended properties> in the context menu to change to the detail form.

Swap to Assignment Details Form



Enter the employee's deputy for this company structure.

Specifying a Deputy



Add Employees to IT Shop Customer Nodes

Tools:
Identity Manager with application role <IT Shop>\<Administrators>
Manager

When employees are added to a customer node, they are authorized to place requests through IT Shop. An employee's overview form shows the IT Shop access permissions and assignments that have been obtained by requesting products via the IT Shop.

Create User Accounts for Employees

Tools:
Identity Manager with application role <Target system>\<Target system manager>
Manager

The overview form displays all the employee's user accounts. You can create new user accounts for the employee in the available target systems using the appropriate task on the assignment form. The input fields on the master data form already contain predefined values. However, you should the default method for creating user account with user account resources. Read section Creating User Accounts with User Account Resources on page 37 for more information.

Direct Assignment of Applications and Resources to Employees

Tools:
Identity Manager with application role <Employees>/<Administrators>
Manager

You can assign company resources directly to an employee when a quick reaction to special requests is needed. This following form are available for this:

- Assign application
  For assigning applications and application packages to an employee.

- Assign resources
  For assigning resources and resource packages to an employee.

You can obtain more information in the section Possible Company Resource Assignments via Roles on page 79.

Assign SAP Permissions

In the Identity Manager, you can add an employee to SAP groups, SAP profiles and SAP roles. The Identity Manager ensures that the right group memberships are created for the employee's SAP user. SAP products are a collection of SAP groups, SAP roles and SAP profiles which result in the respective group memberships of the employee's user accounts when the assignment is made. Read more in section Groups, Profiles and Roles Administration on page 383.

View Sources of Employee Assignments

The company resources and user accounts that an employee uses and their possible path of inheritance are shown on the form <Show sources of inherited assignments>. Here, the difference is taken into account between direct and indirect employee assignments that can result from the employee's membership in company structures.

View Employee's Responsibilites in the Identity Manager

An employee's responsibilities within the Identity Manager are displayed on their overview form. Functions that are included here might be department manager, cost center manager or IT Shop approver, for example.

View and Edit Defined Violations against the Rules

The <Rule evaluation> form shows which identity audit rules the employee has actually violated and whether a rule exception exists. The rules that the employee has not violated are also displayed. You can analyze the rule violations and issue them with exceptions. You can find more detailed information about analyzing and editing rule violations in the section Rule Checking on page 449.

Authorize an Employee to be the Identity Manager Administrator

An employee has to be set up as the Identity Manager administrator to be able to work with the Identity Manager. User the task "Authorize as the Identity Manager administrator" to add the employee to the required Identity Manager permissions roles. The Identity Manager administrator can then log in to the Identity Manager and add more employees to other Identity Manager permissions roles. The task is only available for the system account user "viadmin" and needs to be run once when the system is set up. This procedure is described in section Assigning Application Roles after Initial Database Migration on page 67. The concept of permissions roles is explained in more detail in section The Identity Manager Application Roles on page 62.

Mapping Multiple Employee Identities

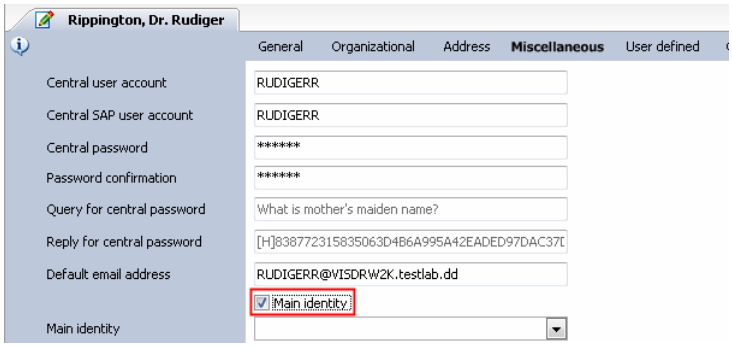
Configuration Parameter for Representing Multiple Identites

CONFIGURATION PARAMETER	EFFECT
QER\Person\MasterIdentity	Preprocessor relevant configuration parameter for controlling the component parts for administrating several identities for one employee. Changes to the parameter require recompiling the database. If the parameter is set, several logical employees can be handled in the database for one physical employee (for example, an employee has different identities and account characterists at different branches).

It might be necessary for employees to have different identities for their work under certain circumstances. For example, identities that result from contracts at different branches. These identities can be differentiated through the membership of a department, cost center or through access permissions. External employees at different locations can also be used and represented with different identities in the system. You can define a main identity and a subidentity for an employee to represent each of the identities and to group them at a central location.

A main identity represents a real person. A main identity does not have its own user account or permissions and may not place and requests for company resources. A main identity can be referenced by several subidentites. The employee master data for a main identity is entered in the Identity Manager. Label the main identity on the employee's master data form with the <Main identity> option.

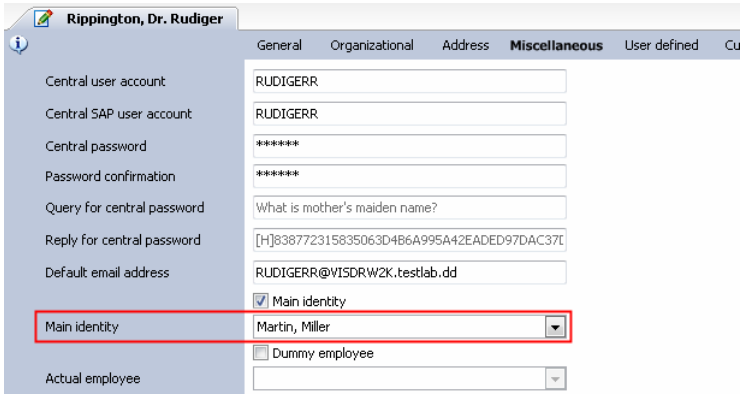
Labling an Employee as Main Identity



A subidentity is a virtual employee. A subidentity can be assigned user accounts and permissions in the Identity Manager and it can place requests in the IT Shop. A subidentity is always linked to a main identity. Employee master data for a subidentity is displayed in the Identity Manager. This can be copied

from the main identity data using the appropriate templates. Enter a main identity for the subidentity using the pop-up menu <Main identity> on the employee's master data form.

Labeling an Employee as a Subidentity



If an employee with multiple identities is being edited despite only one identity being currently known to the Identity Manager, you should create a main identity for that employee. You should assign the previously know identity as a subidentity and create new subidentites for the other identities. In this way, it is possible to test the employee's permitted permissions per subidentity or per main identity including all subidentities in the bounds of an identity audit.

3

The Identity Manager Roles Model

- Introduction
- The Identity Manager Application Roles
- How to Edit Identity Manager Application Roles
- Identity Manager Application Roles for Target System Adminstration

Introduction

In the Identity Manager, you can specify in detail user access permissions via permissions groups. The Identity Manager roles model offers an alternative method of specifying them. The Identity Manager makes so-called application roles available. Application roles are linked to permissions groups with access permissions preset by the Identity Manager. The administration of access permissions is noteably improved by the Identity Manager application roles.

Access permissions are used for controlling:

- Navigation configuration in administration tools,
- Access to objects and their properties,
- Which interface forms and tasks are displayed
- Availability of special program functionality

The role model takes into account technical aspects (i.e. administration rights to the Identity Manager tools) as well as functional aspect that result from the Identity Manager user's tasks within the company (i.e. permission to approve requests).

In the following sections, the Identity Manager application roles are described and you will learn how to create, edit or delete application roles.

The Identity Manager Application Roles

In order for users to use the Identity Manager predefined access permissions they have to log onto the Identity Manager tools with a role base athentication module. The authentication module finds a system account user from all the application roles that a user is assigned to. The access permissions from this system user are added to by the roles and user accounts that a user is assigned to. In this way, Identity Manager users obtain access permissions to Identity Manager functions at login that correspond to their roles.

You can start the following tools with role based authentication:

- Identity Manager
- IT Shop

Identity Manager application roles have the following aims:

- Program functions, employees, company resources, approval workflows and approval policies are assigned to fixed application roles. The access permissions for these application roles do not need to be defined specifically for the company. This simplifies access permission administration.
- Enables audit secure internal administration of Identity Manager users and their access permissions. Permissions can be granted through assignment, requesting and approval or by calculation on account of specific properties. Furthermore, issuing permission through the attestation function is integratedinto the attestation process.

The following application roles are included in the Identity Manager by default. You can assign these application roles to employees and edit them. You cannot delete the default application roles.

Application Roles

CATEGORY	APPLICATION ROLE	PERMISSIONS GROUPS
General	Identity Manager Administrators	vi_4_AEADMIN
	Identity Manager Everyone	vi_4_ALLUSER
	Identity Manager all managers	vi_4_ALLMANAGER
Attestation	Administrators	vi_4_ATTESTATIONADMIN_ADMIN
Identity Audit	Administrators	vi_4_RULEADMIN_ADMIN
	Attestors	vi_4_RULEADMIN_ATTESTATOR
	Rule supervisor	vi_4_RULEADMIN_RESPONSIBLE
	Exception approver	vi_4_RULEADMIN_EXCEPTION
	Maintain SAP Functions	vi_4_RULEADMIN_SAPRIGHTS
IT Shop	Administrators	vi_4_ITSHOPADMIN_ADMIN
	Attestors	vi_4_ITSHOPADMIN_ATTESTATOR
	Product owner	vi_4_ITSHOPADMIN_OWNER
Employees	Administrators	vi_4_PERSONADMIN
Business roles	Administrators	vi_4_ROLEADMIN_ADMIN
	Attestors	vi_4_ROLEADMIN_ATTESTATOR
	Approver	vi_4_ROLEADMIN_RULER
	Approver (IT)	vi_4_ROLEADMIN_RULERIT
Organizations	Administrators	vi_4_STRUCTADMIN_ADMIN
	Attestors	vi_4_STRUCTADMIN_ATTESTATOR
	Approver	vi_4_STRUCTADMIN_RULER
	Approver (IT)	vi_4_STRUCTADMIN_RULERIT
Target system	Administrators	vi_4_NAMESPACEADMIN_ADMIN
	Target system managers	vi_4_NAMESPACEADMIN_ADS vi_4_NAMESPACEADMIN_LDAP vi_4_NAMESPACEADMIN_NOTES vi_4_NAMESPACEADMIN_SAPR3 vi_4_NAMESPACEADMIN_UNS

Identity Manager Administrators

Identity Manager users with this application role can assign employees to any administrator application role. They may add other employees to the application role <Identity Manager administrators> and edit conflicting application roles..

At least one employee must be added to the application role <Identity Manager administrator> straight after the initial database migration.

The following application roles are provided for employee administration:

Identity Manager Everyone

The application role is automatically assigned to each user when they log in with a role based authentication module. Each user can edit their own master data in the IT Shop.
If every user should be automatically assigned to a custom permissions group when they log in then this permissions group can be added to the application role <Identity Manager Everyone>.

Identity Manager all Managers

This application role is automatically assigned to each user when a login takes place with a role based authenication module. It takes effect when the logged in user is responsible for, or a manager of emplyoees, departments, locations, cost centers, business roles or IT Shops. Identity Manager users with this application role can edit master data for the objects they are responsible for and assign company resources to them.
Identity Manager users with the application role <Identity Manager all managers> can edit their employee‘s master data in the IT Shop.

Administrators

Administrators can edit the master data of all employees. They specify the primary department, primary cost center or the primary location for an employee. However, assigning employees to additional departments, cost centers , locations or other structures for this application role is not permitted.

Employees

The following application role is available for employee administration:

- Administrators
  Identity Manager users with this application role can edit master data for all employees and assign company resources to them.

Organizations

The following application roles are available for the administration of departments, cost centers and locations:

- Administrators
  Identity Manager users with this application role can edit the master data for all departments, cost centers and locations and assign company resources to them.
  They assign employees to the other application roles in the ‘Organizations‘ category. They can define child application roles and edit conflicting application roles. Administrators can assign the rest of the application roles to custom defined permissions groups.

- Attestors
  Identity Manager users with this application role attest company resource assignments to departments, cost centers and locations that their application role is assigned to.

- Approvers
  Identity Manager users with this application role also belong to the IT Shop approvers. They can approve requests from their staff from department, cost centers and locations that their application roles are responsible for. You can view but not edit the master data and assignments for these organizations.

- IT Approvers
  Identity Manager users with this application role also belong to the IT Shop approvers for the IT Shop. They can approver requests from their staff from department, cost centers and locations that their application roles are responsible for.

Business Roles

The following application roles are available for the administration of business roles:

- Administrators
  Identity Manager users with this application role can edit the master data for all business roles and assign company resources to them.
  Identity Manager users with this application role assign employees to the other application roles in the 'business roles' category. They can define child application roles and edit conflicting application roles. Administrators can assign the rest of the application roles to custom defined permissions groups.

- Attestors
  Identity Manager users with this application role attest to the correctness of company resource assignments to the business roles that their application role is assigned to.

- Approvers
  Identity Manager users belonging to this application role also belong to the IT Shop approvers. They can approver requests from their staff from business roles that their application roles are responsible for.

- IT Approvers
  Identity Manager users belonging to this application role also belong to the IT Shop approvers for the IT Shop. They can approve requests from their staff from business roles that their application roles are responsible for.

IT Shop

The following application roles are available for the IT Shop administration:

- Administrators
  Identity Manager users with this application role can edit the entire IT Shop structure (shop, shelves, approval policies, templates, service catalog) and assign products. They set up and edit service items. Furthermore, they decide, which company resources can be requested from the IT Shop.
  Identity Manager users with this application role assign employees to other application roles in the IT Shop category. They can define child application roles and edit conflicting application roles. Administrators can assign the rest of the application roles to custom defined permissions groups.

- Attestors
  Identity Manager users with this application role attest to the correctness of company resource assignments to the IT Shop that their application role is assigned to. Furthermore, they attest the validity of service items. They can view master data and assignments these IT Shop structures and service items but are not permitted to edit them.

- Product owners
  Identity Manager users with this application role also belong to the IT Shop approvers. They can approve requests for service items that their application role is assigned to. They can edit the master data for these service items and assign company resources to them.

Identity Audit

The following application roles are available for compliance rule administration:

- Administrators
  Identity Manager users with this application role edit the working copies of all compliance rules. Assign mitigating control to them and enable or disable the rules. Furthermore, they define SAP functions and assign these to managers (Identity Manager users with the application role <Maintain SAP functions>. They define function instances and variable sets for SAP functions and enable the working copies.
  Identity Manager users with this application role assign employees to the remaining application roles in the category <Identity Audit>. They can define child application roles and edit conflicting application roles. Administrators can assign the rest of the application roles to custom defined permissions groups.

- Attestors
  Identity Manager users with this application role attest to the validity of compliance rules or exception approvals that their application role is assigned to. They can view the master data for these compliance rule but not edit it.

- Rule supervisor
  Identity Manager users with this application role edit working copies of the compliance rules that their application role is assigned to. They assign mitigating controls and enable or disable the rules.

- Exception approver
  Identity Manager users with this application role edit compliance rule violations for which they are entered as exception approver.

- Maintain SAP functions
  Identity Manager users with this application role can edit the working copies of SAP functions that are assigned to their application role. They define function instances and variable sets fir these SAP functions and can enable working copies.

Attestation

The following application roles are available for the attestation procedure administration:

- Administrators
  Identity Manager users with this application role define and monitor attestation processing.

Target System

The following application roles are available for target system administration:

- Administrators
  Identity Manager users with this application role can allocate employees to the remaining roles in certain target systems. They can define child application roles and edit conflicting appliction roles. Administrators can assign the rest of the application roles to custom defined permissions groups.
  Identity Manager users with this application role only manage the application roles for each target system. They do not take on any administrative tasks within the target system.

- Target System Managers
  Identity Manager users with this application role assume the administrative tasks within each target system. There is at least one application role per target sytem. The target system managers can create, change or delete target system objects, such as user accounts, user account groups or container structures in Identity Manager.

- You edit the master data with the Identity Manager.
- You user the IT Shop to attest, approve requests, approve rule violations, edit your own employee master data, make request in IT Shop.

How to Edit Identity Manager Application Roles

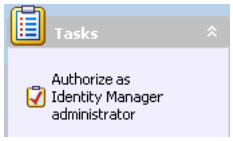
Assigning Application Roles after Initial Database Migration

In order to edit application roles, you must add one employee in the application role ”Identity Manager Administrators“ after initial migration. Proceed as follows:

1. Start the Manager with the system user ”viadmin“.
2. Select the category <Employees>.
3. Select the employee to be assigned to the application role from the result list.
4. Open master data or the overview form.
5. Run the task <Authorize as Identity Manager administrator>.

This assigns the employee to the application role <Identity Manager Administrators>. As soon as you refresh the Manager view, the task <Authorize as Identity Manager Administrator> is no longer shown in the task view. That means that the task can only be run when there are no other employees assigned to this application role.

Authorize Employee as First Identity Manager Administrator



It is possible that no more employees assigned to the application role <Identity Manager Administrators> after you have been working with Identity Manager for a while. In this case, proceed as described above in order to reassign an employee to this application role.

The Identity Manager users with the application role <Identity Manager Administrators> can now add more employees to application roles and edit the application role master data. To do this, the administrator logs on the Identity Manager using a role based authentication module. Read the following sections to find out how to assign employees to application roles and edit the master data.

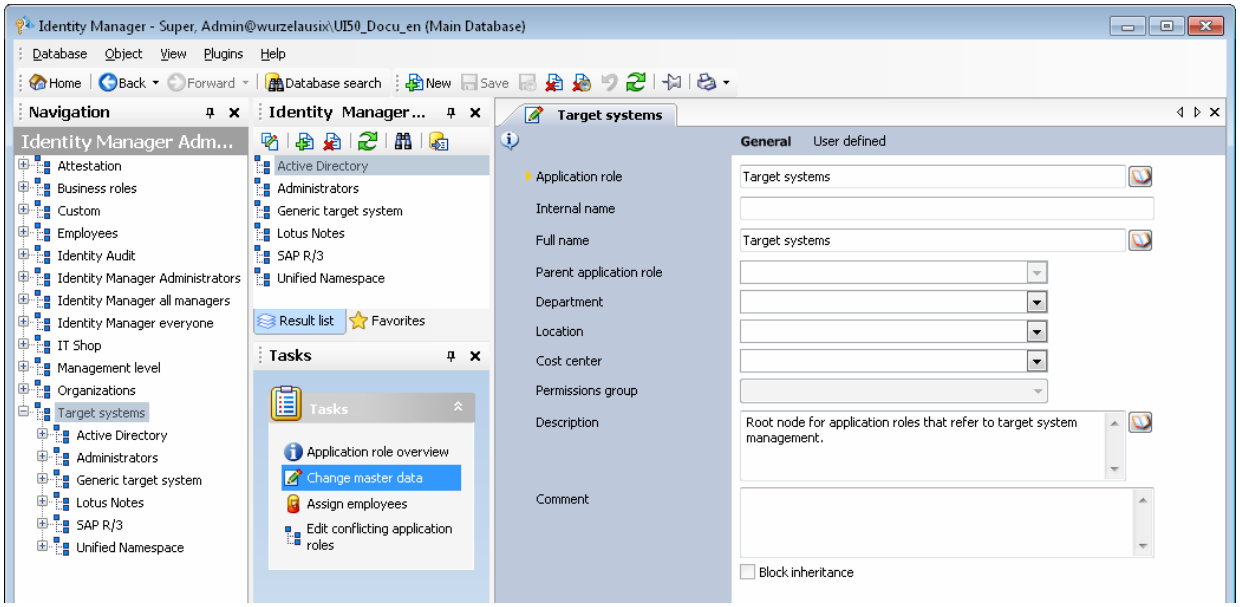
How to Edit Master Data

To edit the application role master, you need to log into the Identity Manager with a role based authenication module. Application roles are grouped by category in the navigation cateogry <Identity Manager Administration>. Only the application roles that you are permitted to edit corresponding to your own application role are shown- You can edit existing application role or add new ones to the hierarchy.

General Master Data

On the <General> form you can edit all the general master data for an application role. If you add a new application role, you must fill out the compulsory fields.

Application Role General Data



Enter the following data:

- Application role
  Name for the application role

- Internal name
  Emtpy text field for a internal company identitfier

- Full name
  Is made up automatically from the application role name and the parent application role.

- Parent application role
  Application role that application role being edited is subordinate to.

- Department, location, cost center
  Additional information for the application role definition.

- Permissions group
  The application role is given the access permissions of the associated permissions group. If there is no permissions group assigned, the application role gets edit permissions from the parent application role.
  Administrators can assign the rest of the application roles to custom defined permissions groups. The permissions group for the application roles <Administrators> and <Identity Ma-

nager administrators> cannot not be edited however.
You can find details about permissions groups in the section System Users and Permissions Groups on page 105 in the Configuration Manual.

- Description, Comment
  Empty text fields for your own use.

Identity Manager users that are logged in with an <Administrator> application role, can add subordinate application roles and assign employees to them there. You can also enter additional information for the application roles in the input fields <Department>, <Location> and <Cost center>. These input fields are only used for information. They do not indicate which organization the application roles are responsible for.

Application roles do not come into effect for the assigned employees until you have assigned objects. You assign the application role on the master data form for the respective object. This applies for all application roles except administrators.

User Defined Master Data

This tab is provided in order to enter additional company specific information to an application role. You can customize the display name, format and template rules for the input fields (by default <Spare field no. 1> to <Spare field no. 10> with Designer to meet your requirements.

Additional Tasks for Managing Application Roles

As soon as the master data for an application role has been entered, you can apply several different tasks to them. Use the overview form to get the most important information about an application role. Furthermore, you can select the tasks described in the following in the task view.

Assign Employees

Use this task to assign employees to application roles and to remove existing assignments. The assigned employee obtain all the access permissions of the permissions group that the application roles is assigned to. Therefore, if you assign employees to an application role, check that the application role has a permissions group assigned to it. Otherwise the assigned employees do not get any role dependent access permissions.

Application roles inherit employee assignments from their parent application role as long as the application role is not directly assigned to an employee.

How to Edit Conflicting Application Roles

Configuration Parameters for Editing Mutually Exclusive Roles

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Structures\DBModel\ExcludeStructures	Preprocessor relevant configuration parameter for controlling the model parts that specify conflicts between roles. After changing the parameters you have to compile the database. If the parameter is set, you can specify which roles are mutually exclusive.

Use this task to specify which application roles are mutually exclusive. You may not assign these application roles to the same employees. Parent nodes definitions do not have any influence on subordinate application roles.

Example:

Exception approvers for rule violations should not be rule supervisor at the same time.
Run the task <Edit conflicting application roles> on the application role <Identity Audit>\<Exception approver> and assign the application role <Identity Audit>\<Rule supervisor>.
Now you will not be able to add employees that are assigned to the application role <Exception approver> to the application role for a rule supervisor. And you cannot add employees that are assigned to the <Rule supervisor> application role to the <Exception approver> application role.

Identity Manager Application Roles for Target System Adminstration

Select a target system manager from the navigation node <Target systems>/<target system>. Identity Manager provides one application per target system by default.

Target system managers for the Unified Namespace can modify all objects that are shown in the category <Unified Namespace>. That means they can modify their own target systems, which are only mapped in the Unified Namespace, as well as the target system Active Directory, Lotus Notes, SAP R/3 and LDAP.

If you want to limit access permissions for Unified Namespace target system managers to single target system, define child application roles and proceed as follows:

1. Login to the Identity Manager with a role based authentication module from the application role <Target systems>\<Administrators>.
2. Add a new application role for each target system.
3. Assign the permissions group vi_4_NAMESPACEADMIN_UNS and the parent application role ”Unified Namespace“ to these application roles.
4. Assign employees to these application roles.
5. Assign the respective target system type to the application roles.

Read the section Setting Up Target System Types in the Unified Namespace on page 135 about how to edit target system types.

You can use the target system managers for Active Directory, generic target systems, Lotus Notes, LanMan and compatible administration and SAP R/3 when you manage them ”fully“ via Identity Manager and the appropriate configuration parameters are set. Target system managers for individual target

system can modify all the objects in the categories <Active Directory>, <Generic target system>, <Lotus Notes> and <SAP R/3>. Assign target system managers for the target system domains or clients. For more detailed information refer to the chapters Managing an Active Directory Environment on page 201, Managing a Lotus Notes Environment on page 295, Managing an SAP R/3 Environment on page 343, Managing Generic Target Systems on page 399.

If you want to limit access permissions for target system managers to individual domains or clients, define subordinate application roles for each target system.

4

Company Structures as Roles in the Identity Manager

- Introduction
- Basics for Creating Roles
- Assigning Company Resources through Roles
- Basic Data for Constructing Roles
- Business Roles
- Departments
- Cost Centers
- Locations
- Additional Tasks for Managing Roles
- Setting Up IT Operating Data
- Working with Dynamic Roles

Introduction

One of the Identity Manager's goals is to provide company employees with the company resources, to ensure an efficient working environment. To do this, the Identity Manager company structures are represented in hierarchical role form.

The term "Roles" is used to bring the company structures departments, cost centers, locations and business roles under one umbrella. Departments, cost centers, locations and business roles are each mapped to their own hierarchy under the heading "Organizations". This is due to their special significance for daily work schedules in many companies. Business roles map company structures with similar functionality that exist in addition to departments, cost centers and locations, project groups for example.

Various company resources can be assigned to roles, for example, authorizations in different SAP systems or access to particular directories and associated applications. Employees can be assigned to these roles. Employees can obtain their company resources and entitlements via these assignments when the Identity Manager is appropriately configured.

Basics for Creating Roles

Roles can either be created following the top-down or the bottom-up model in the Identity Manager. In the top-down model, roles are defined based on the area of activity and the entitlements required to fulfill the activities are assigned to the roles. In the case of the bottom-up model , permissions assignments are analyzed and the roles result from this.

Roles can be hierarchically allocated. Entitlements and company resources can be passed on through inheritance over the hierarchies. In this case both inheritance directions "top-down" and "bottom-up" may be implemented.

In the following, the basics are explained for distributing company resources via hierarchical roles. The internal flow of inheritance and inheritance rules for individual company resources are descibed in the Configuration Manual, chapter Identity Manager Inheritance on page 275.

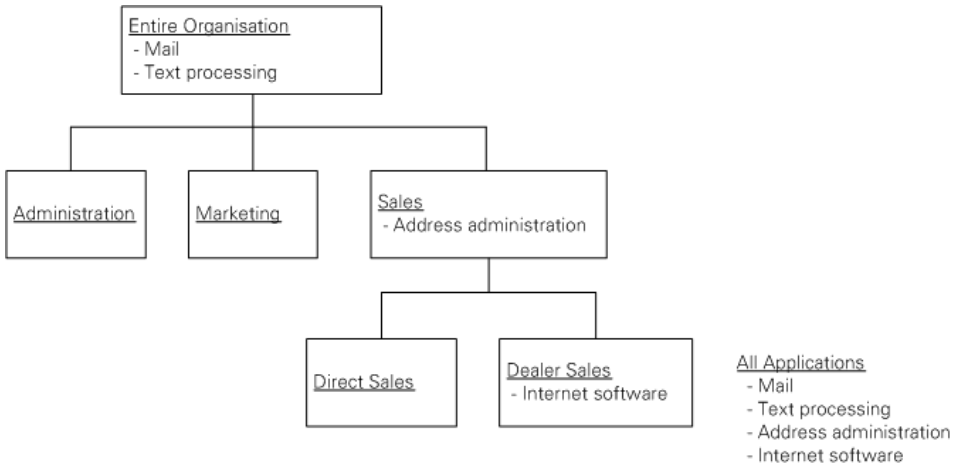
Direction of Inheritance within a Hierarchical Role Structure

Distribution of company resources is decided by the direction of inheritance within a hierarchical of roles. The Identity Manager is basically aware of two directions of inheritance - "top-down" and "bottom-up". The effects on the allocation of company resources is explained in the following example for assigning an application.

In the Identity Manager, the default structure within a company is called put into effect through "top-down" inheritance. With its help, a company's multilevel form can be represented with main departments and respective subdepartments. Application assignments can be seen in the following diagram. In the diagram above a section of a company's structure is illustrated. The respective applications assigned to the departments are also shown. An employee in retail is assigned all the applications that are

allocated to his or her department and all those on the full structure path. In this case that is internet software, address administration, mail and text editing.

Application Assignment via ”Top-Down“ Inheritance



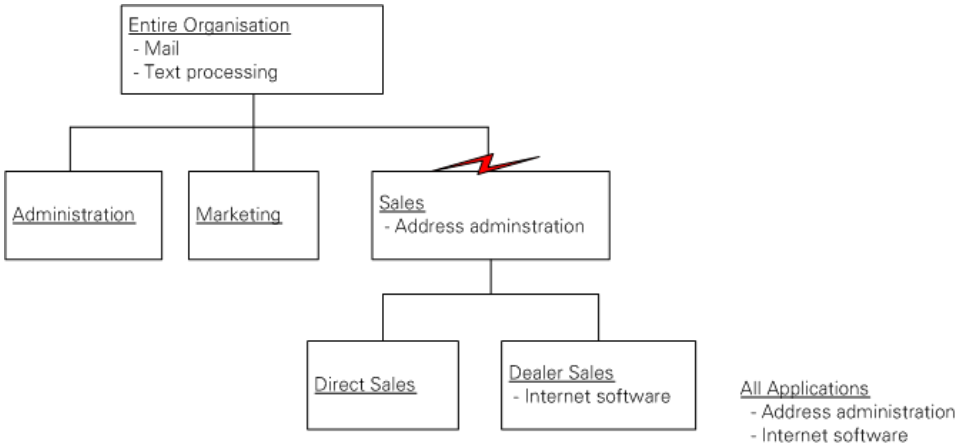
With ”top-down“ inheritance, assigments are inherited in the direction of more detailed classifications where as ”bottom-up“ inheritance operation in the other direction. This inheritance direction was introduced to map project groups in particular. The aim being, to provide a coordinator of several project groups with the resources that each of the project group deals with.

Discontinuing Inheritance

There are particular cases where you may not want to have inheritance over several hierarchical levels. That is why it is possible to discontinue inheritance within a hierarchy. The point at which the inheritance should be discontinued within a hierarchy is specified by the option <End inheritance>. The effects of this depend on the chosen direction of inheritance.

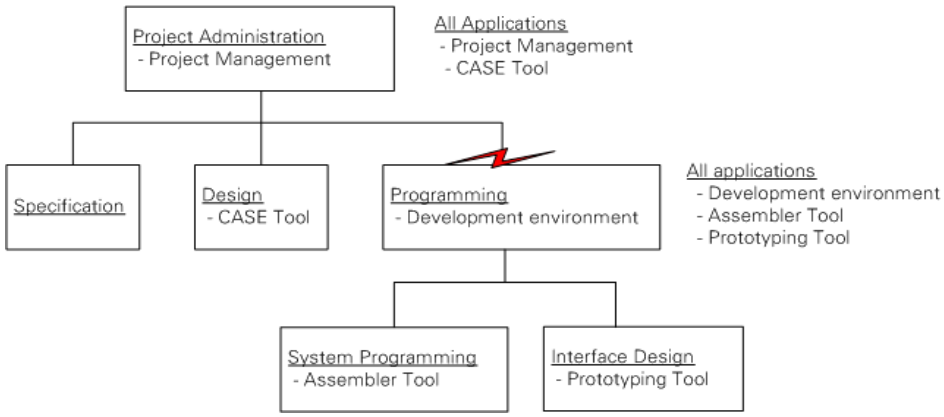
The role labeled with this option in ”top-down“ inhertance, cannot inherit assignments from higher levels. It can, however, pass on its own directly assigned company resources to lower level structures. If the option <End inheritance> is set for the department ”Sales“ in the example below, it results in sales employees being assigned address administration and employees in the retail department, address administration and internet software, but neither is assigned mail or text editing applications..

Discontinuing Inheritance ”Top-Down“



In ”bottom-up“ inheritance, the role labeled with this option inherits all assignments from lower levels in the hierarchy. However, it does not pass any assignments further up the hierarchy. The next figure shows ”bottom-up“ inheritance based on a project framework. An employee from the project group ”Programming“ receives the applications from the project group as well as those from the projects groups below. In this case, the development environment, assembler tool and the prototyping tool. The project group ”Programming“ is given the option <End inheritence>. That means that it does not pass assignments on. The result being that the project leaders along with the application project management are only assigned the CASE Tool. The applications from the projects groups ”Programming“, ”System programming“ and ”Interface design“ are not distributed to the project leaders.

Discontinuation of Inheritance ”Bottom-Up“



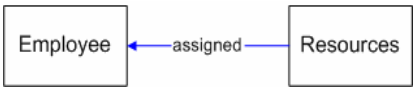
Possible Assignment Types

In the Identity Manager, company resources can be assigned to employees. There are different ways to assign company resources - by direct and indirect assignment. The indirect way of assigning company resources is subdivided into primary and secondary assignment.

Direct Assignment

Direct assignments can be made, for example, by entering user accounts directly in a group or by allocating an application or a resource to an employee. Direct assignment of company resources makes it easier to react to special requirements.

Direct Inheritance Schema

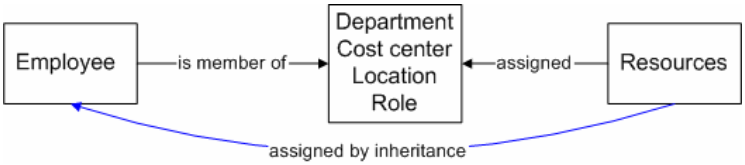


Indirect Assignment

When company resource are indirectly assigned, employees are allocated to departments, cost centers and locations or business roles. The total of assigned applications, groups and resources for the employee is calculated from the position within the hierarchies, the direction of inheritance (top-down or bot-

tom-up) and the company resources assigned to these roles. Indirect assignment is the default method for distributing company resources because of the ease of administration.

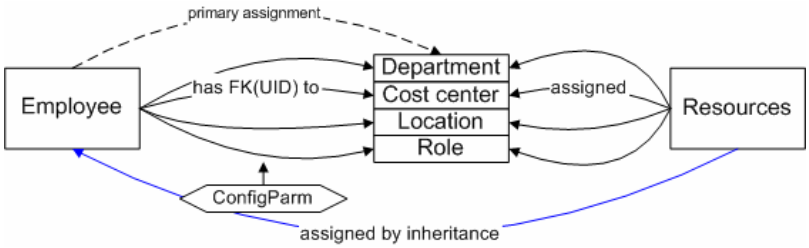
Indirect Inheritance Schema



Primary Assignment

Primary assignment takes place by referencing a business role, department, cost center or location via a foreign key to the employee. Use the input fields for roles on the master data form for employees, hardware or wordesks to do this. Primary assignment inheritance can be activated over configuration parameters. When the configuration parameters are changed the inheritance is recalculated. Primary assignment is enab led by default for employee objects.

A Primary Assignment Schema



Changes to the configuration parameter result in the inheritance data being recalculated! That means that if the primary assignment is disabled at alater date, the inheritance data created in this way will be removed from the database.

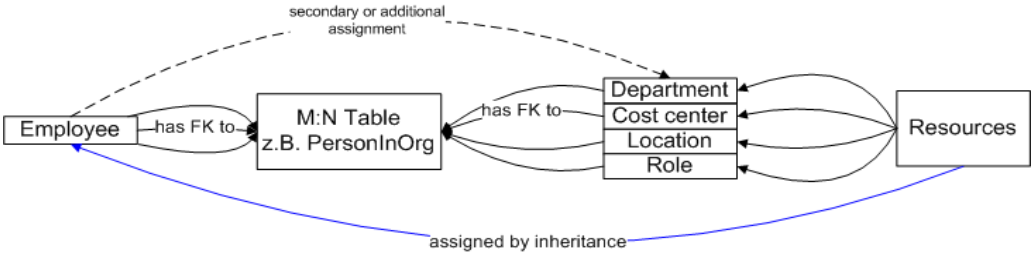
Configuration Parameters for Primary Assignment

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Structures\Inherite\Person	Employees can inherit by primary assignments.
QER\Structures\Inherite\Person\FromDepartment	Employees inherit assignments of their primary department (Person.UID_Department). Default!
QER\Structures\Inherite\Person\FromLocality	Employees inherit assignments of their primary location (Person.UID_Locality). Default!
QER\Structures\Inherite\Person\FromOrg	Employees inherit assignments from their primary business role (Person.UID_Org). Default!
QER\Structures\Inherite\Person\FromProfitCenter	Employees inherit assignments from their primary cost center (Person.UID_ProfitCenter). Default!

Secondary Assignment

Secondary assignment takes place by assigning an employee from an role. To do this, run the additional task <Assign employees> to the role. Secondary assignment is the default method for assigning and inheriting company resources through roles. Use the role classes (department, location, cost center, business role) to specify whether a secondary assignment to company resources is possible. In the process, you define whether direct assignment is possible. If direct assignment is not possible, the employee objects are assigned to the roles via an approved request.

Secondary Assignment Inheritance Schema



Secondary assignments are mapped in the table PersonInBaseTree.

Assigning Company Resources through Roles

The level of assignment and inheritance of company resources via roles depends on particular properties of the affected objects. You should take these into account when setting up your company structures.

Sorting Employees into Roles

Use the role classes to specify the company resources that are permitted to have assignments to roles belonging to these role classes. You also define whether direct assignment is possible for these company resources. You have to allow the assignment of employees to role classes so that they can inherit company resources via secondary assignment.

To do this you use the following input fields:

- Assignment permitted for
  Select the company resources in the drop-own menu that are available for making a secondary assignment to a role from a role class.
  You can only disable a company resource as long as no secondary assignments exist or can be added via existing dynamic roles.

- Direct assignment permitted for
  Select the company resources in the drop-own menu that are available for making a direct assignment to a role from a role class. Company resources that are not selected here can only be assigned via approved IT Shop requests. Company resources permitted direct assignment are automatically enabled in the input field <Assignments permitted for>.
  You can only disable a company resource if it does not have any direct assignments.

Assignments and direct assignments are permitted by default for the role classes department, cost center and location.

Specifying the Direction of Inheritance for Roles

The direction of inheritance within a hierarchy of roles is decided by the distribution of company resources. The effect of the selected inheritance direction on the assignment of company resources is described in more detail in section Direction of Inheritance within a Hierarchical Role Structure on page 74.

Specify the inheritance direction within the hierarchy with the role class option <Inherited top down>. The inheritance direction applies to the whole hierarchy that is based on this role class. You must enable this option to provide ”top-down“ inheritance and disable it for ”bottom-up“ inheritance. This option is set by default for departments, cost centers and locations which means ”top-down“ inheritance takes place.

There are particular cases where you may not want to have inheritance over several hierarchical levels. That is why it is possible to discontinue inheritance within a hierarchy. The point at which the inheritance should be discontinued within a hierarchy is specified by the option <End inheritance>. The effects of this depend on the chosen direction of inheritance. See section Discontinuing Inheritance on page 75 about the effects of this option.

Using Roles to Limit Inheritance

In order to temporarily prevent employees from inheriting company resources for specific roles, use the option <Employees do not inherit>.

If the options are set, employees in this role do not inherit. This means that you can make all the necessary assignments to a role. Inheritance of company resources does not take place, however, until the role options are disabled, for example, after running through a defined approval process.

You can prevent employees from inheriting company resources entirely by setting the option <No inheritance>. If this option is set, employees cannot inherit any company resources via roles. This means that you can make corrections after importing employees, for example, and then reactivate company resource inheritance by disabling the option. This option not relevant for direct assignment.

Possible Company Resource Assignments via Roles

Employees can inherit company resources via indireect assignment. For this, employees can be members of as many roles as required. When new company resources have been assignment the DBScheduler recalculates the inheritance data. Employees obtain the necessary company resources via defined inheritance rules. The inheritance rules are explained in more detail in the Configuration Manual, in chapter Identity Manager Inheritance on page 275.

Roles can be defined:

- Unified Namespace system entitlements
  Read section Additional Tasks for Managing System Entitlements on page 156 about setting up groups in the Unified Namespace.

- Active Directory groups
  Read section Entering Master Data for Active Directory Contacts on page 241 about setting up Active Directory groups.

- Lotus Notes groups
  Read section Lotus Notes Groups on page 330 about setting up Lotus Notes groups.

- LDAP groups
  Read section LDAP Groups on page 418 about setting up LDAP groups.

- SAP groups, SAP roles and SAP profiles
  Read section Groups, Profiles and Roles Administration on page 383 about setting up SAP groups, SAP roles and SAP profiles.

- Structural profiles
  Read section Managing Structural Profiles on page 391 about customizing structural profiles.

- Resources
  Read the section Editing Resources on page 108 about creating resources.

- Applications
  Read the section Setting Up Applications on page 124 in the Service Management Manual about setting up applications.

- System roles
  Read the section System Roles on page 114 about about setting up system roles.

Inheritance Exclusion

Configuration Parameter for Conditional Inheritance

CONFIGURATION PARAMETER	EFFECT WHEN ENABLED
QER\Structures\Inherite\GroupExclusion	Preprocessor relevant configuration parameter for controlling inheritance of group memberships.Changes to the parameters requires recompiling the database. If the parameter is set you can exclude target system groups and system entitlements from inheritance.

It might be possible for an employee to obtain more than one target system group (system authorizations) through different roles in an invalid combination by indirect inheritance of target system groups and system authorizations to user accounts in the unified namespace. To prevent this, you define inheritance exclusion. This means that you specify which of two target system groups (system authorizations) should be inherited by the user account if both are assigned. When inheritance is calculated the DBScheduler only creates an entry in the corresponding Total table for this target system group (system authorizations). For detailed information about calculating inheritance see section Identity Manager Inheritance on page 275 in the Configuration Manual.

Prerequisites:

- The configuration parameter ”QER\Inherite\GroupExclusion“ is enabled.
  This configuration parameter is preprocessor relevant. After changes have been made to it you need to compile the database. See sections Compiling an Identity Manager Database on page 100 in the Getting Started Manual and Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual for more information.

- Mutually exclusive target system groups (system authorizations) belong to the same target system area.

Procedure:

1. Run the task <Specify inheritance exclusion> for the target system group (system authorizations) that is going to be inherited.

2. Assign the target system group (system authorizations) that is excluded from inheritance.

Example:

An SAP role A in an SAP system has authorizations defined to trigger requests. An SAP role B authorized to make payments. An SAP role C authorized to check invoices. SAP role A is inherited by the SAP user through department Z1, role B through department Z2. SAP role C is inherited through business role G. An employee with user account K in this SAP system belongs primarily to the department Z1. The business role G and department Z2 are assigned secondarily to the employee. Without inheritance exclusion the SAP user account K obtains all the authorizations of SAP roles A, B and C (entries in SAPUserInSAPGroupTotal for all three roles).

By using suitable means, you want to prevent an employee from being able to trigger a request and to pay invoices. An employee that check invoice should also not be able to make payments. Inheritance exclusion is defined for SAP roles B and C in order to do this.

Resulting Assignments for SAP User Account K - 1

ROLE	ASSIGNED SAP GROUP <BASETREE>HASSAPGROUP-TOTAL	EXCLUDED SAP GROUP	THROUGH INHERITANCE ASSIGNED SAP GROUPS SAPUSERINSAPGROUPTOTAL
Z1	SAP role A		
Z2	SAP role B	SAP role A	
G	SAP role C	SAP role B	SAP role C

The DBScheduler deletes the SAP role assignments A and B from the table SAPUserInSAPGroupTotal through inheritance exclusion. Only the assignment of the SAP role C remains in the table SAPUserInSAPGroupTotal and is declared in the SAP system. If the assignment of the business role G to the employee is removed at a later date, the SAP role B is reassigned to the user account.

Only direct defined inheritance exclusion between target system groups (system authorizations) are taken into account!

If the employee is only a member of department Z1 and the business role G, the SAP role A and C assignments remain because there was no direct inheritance exclusion defined between these SAP roles. That means that the employee is authorized to trigger request and to check invoices. If this should not be allowed, define further inheritance exclusion for the SAP role C.

Resulting Assignments for SAP User Account K - 2

ROLE	ASSIGNED SAP GROUP <BASETREE>HASSAPGROUP-TOTAL	EXCLUDED SAP GROUP	THROUGH INHERITANCE ASSIGNED SAP GROUPS SAPUSERINSAPGROUPTOTAL
Z1	SAP role A		
G	SAP role C	SAP role B SAP role A	SAP role C

Inheriting Group Memberships Based on Categories

User accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified by a template. Each category is given a specific position within the template. Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. If at least one of the category position between user account and assigned group matches, the user account inherits the group. If the group or the user account is not classified in categories, the user account inherits the group as well.

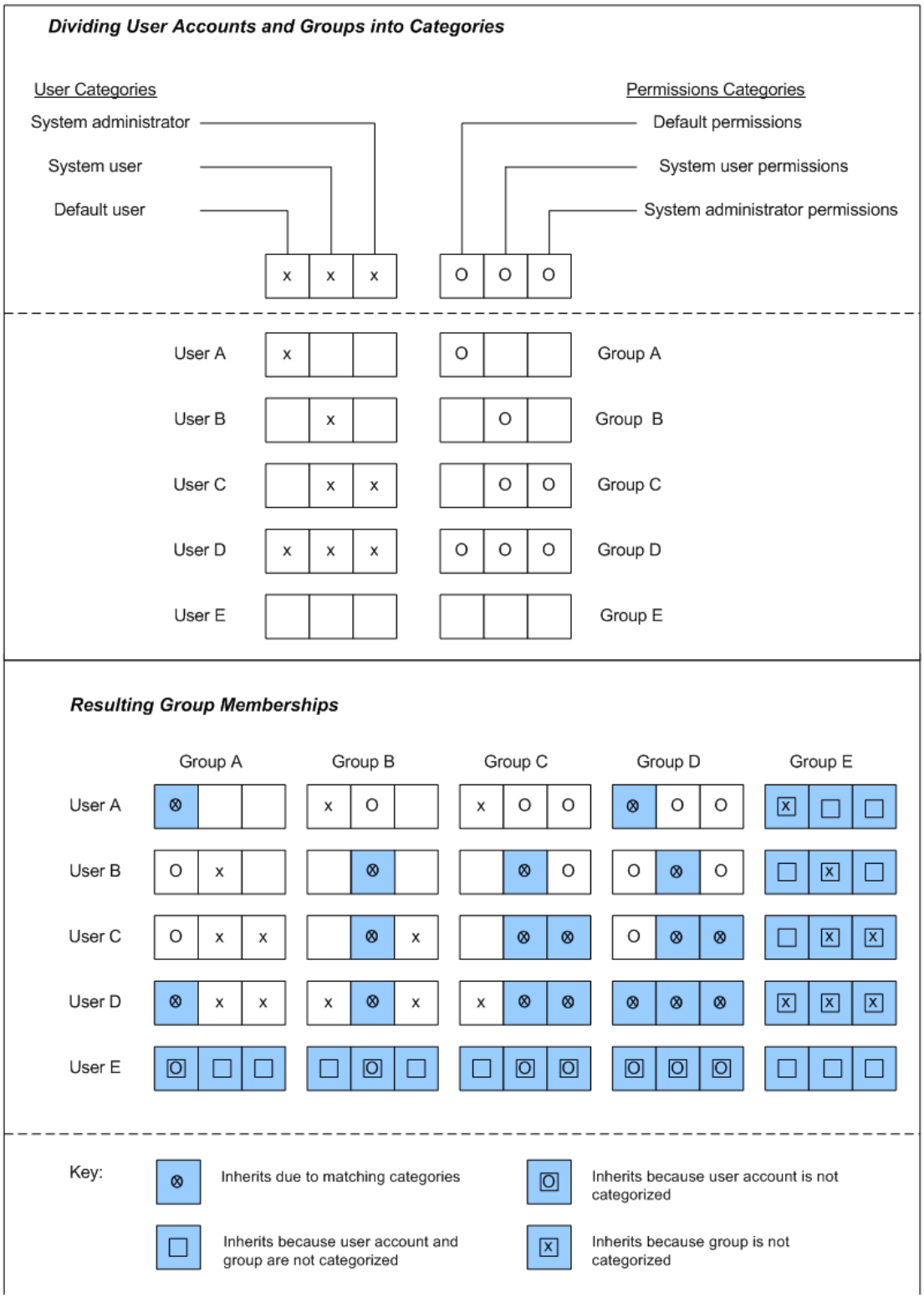
Category Examples

CATEGORY POISITION	CATEGORIES FOR USER ACCOUNTS	CATEGORIES FOR GROUPS
1	Default user	Default permissions
2	System user	System user permissions
3	System administrator	System administrator permissions

You can set up categories for every target system area of the implemented target system, for different domains in an Active Directory environment, for example. For more information, read the section about setting up target system components (Configuration of Extended Properties for an Active Directory Domain on page 212, Specifying Categories on page 354).

Inheritance via categories can only take place by indirect assignment of groups through business roles, departments, cost centers and locations. Categories are not taken into account when groups are directly assigned to user accounts.

Example for Inheriting a Group via Categories



Basic Data for Constructing Roles

Role classes create the basis for building up hierarchical roles in the Identity Manager. These are used to group similar roles together. The inheritance direction for a hierarchy is defined through the role class.

The following role classes are available by default in the Identity Manager.

Default Role Classes inthe Identity Manager

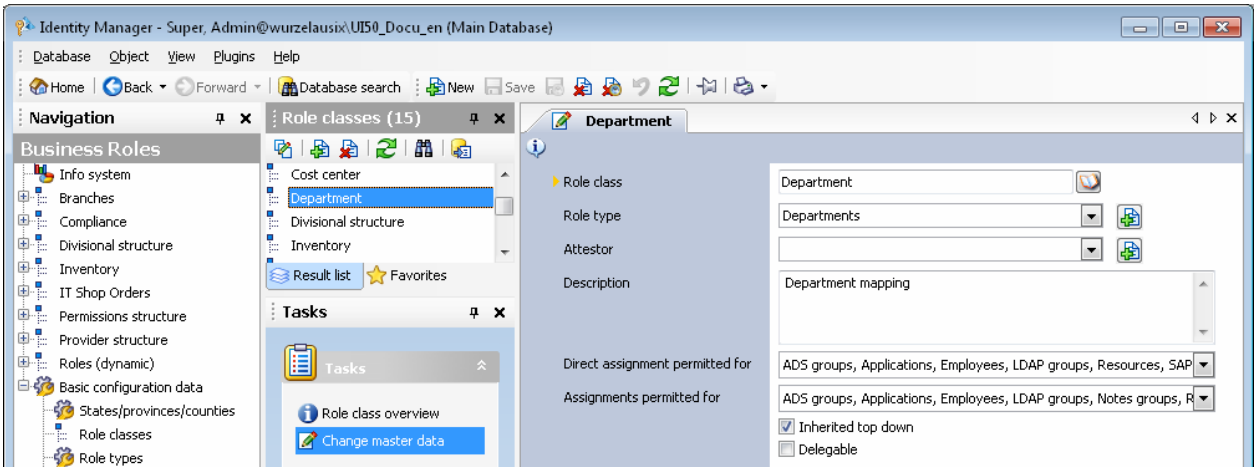
ROLE CLASSES
Department
Identity Manager application roles
IT Shop structure
IT Shop template
Cost center
Rule violation
Location

You can use role types, levels and functional areas for further role structuring. Role types are used to map roles in the user interface, for example. Levels can used to make further subdivisions within the role types.

Role Classes

Modify role classes in tIdentity Manager in the category <Business Roles>\<Basic configuration data>\<Role classes>. Login with a role based authenication module from the application role <Business Roles>\<Administrators>. You can also edit role classes in the Manager.

Setting up a Role Class



Enter the following master data for a role class:

- Role class
  The role classes are shown by these name under the category <Business Roles>.

- Role type
  A role type is used for further subdivision of various role classes.

- Attestor
  Applications role whose members are authorized to approve attestation instances for all roles in this role class. The input field for this is only visible if the configuration parameter ”QER\Attestation“ is set. You can find detailed information about attestation in the section Attestation and Recertification on page 471. For more information about the application role <Attestor> see section Application Roles on page 87.

- Desription
  Empty field for your description

- Direct assignment permitted for
  Mark the company resource in the drop-down menu that should be possible to directly assign to a role of this role class. Company resources that are not selected here, can only be assigned via an IT Shop approved request. Company resources can be assigned directly are already enabled in the <Assignment permitted for> list. For more information read the section Sorting Employees into Roles on page 78.
  You can disable company resources as long as there are no direct assignments associated with it.

- Assignments permitted for
  Mark the company resource in the drop-down menu that may be secondarily assigned to a role of this role class. Read more in section Sorting Employees into Roles on page 78.
  You can disable company resources as long as there are no secondary assignments associated with it and they cannot be added via dynamic roles.

- Direction of inheritance
  Specify the direction of inheritance within a role structure with the option <Inherited top-down>. The direction of inheritance Is valid for the complete role structure that is based on this role class. You have to set the option to map ”top-down“ inheritance or leave it unset for ”bottom-up“. The effect of the chosen direction of inheritance is described in more detail in the section Direction of Inheritance within a Hierarchical Role Structure on page 74.

- Delegable
  Specifies whether you can delegate secondary membership in roles belonging to this role class. Basically, membership in role classes - Identity Manager application roles, departments, cost centers, locations, business roles, IT Shop structure is delegable. If you disable the option on one of these role classes, you cannot select this object class for delegation in IT Shop. For more information read the section Preparing to Delegate on page 51 in the IT Shop Manual.

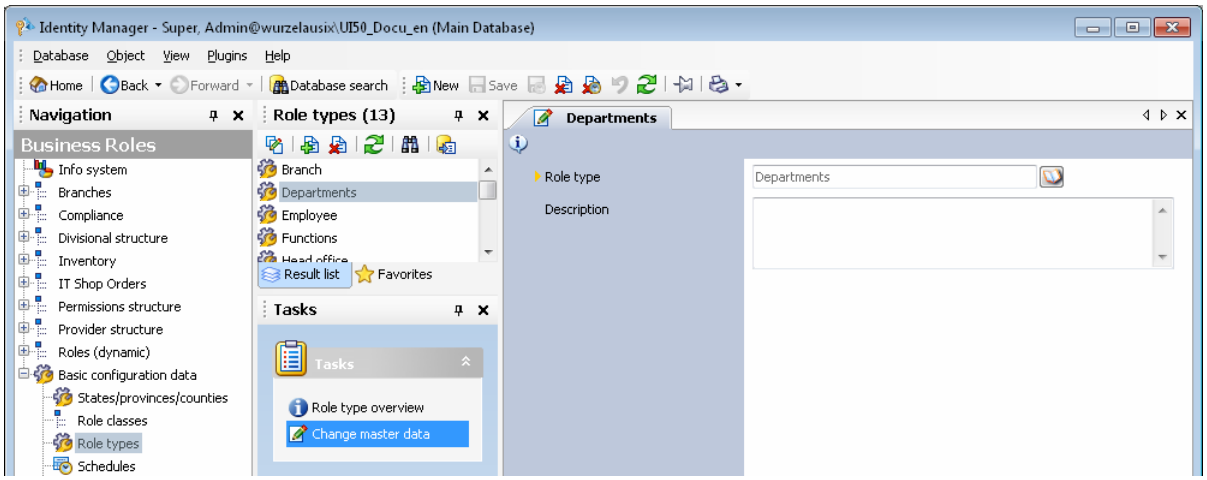
You cannot delete the default role classes. However, you can edit their master data.

Role Types

Create role types in order to classify roles. Roles types can be used to map roles in the user interface, for example. You can enter structure types in the category <Business Roles>\<Basic configuration data>\<Role classes>. To do this you have to log on to the system with a role based authentication

module in the application role <Business roles>\<Administrators>". You can also edit role types in Manager. Enter a name and description for the role type.

Setting up a Role Types



Functional Areas

You need to set up functional areas in order to analyse rule checks for different roles in the context of identity audit. Assign functional areas to departments, cost centers, locations or business roles. You can enter criteria that provide information about risks from rule violations for functional areas and roles. To do this, you specify how man rule violations are permitted in a functional area or a role. You can enter separate assessment critera for for each role, such as a risk index or transparency index. Read the section Rule Compliance in the Identity Manager on page 421 for more information.

Example:

The risk of rule violation in project groups should be analysed. Proceed as follows:

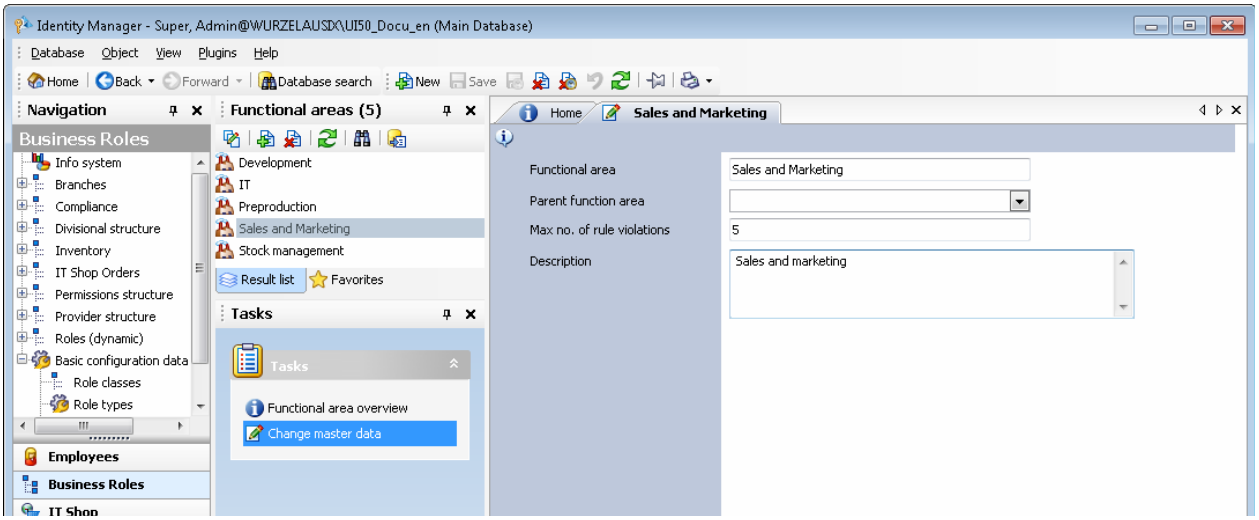
1. Set up a functional area
2. Assign the functional area to business roles that map the project groups in the Identity Manager
3. Define assessment criteria for the business roles
4. Define assessment criteria for the functional area
5. Assign the functional area to the compliance rules that it is relevant for

Use the Identity Manager report function to create a report that prepares a report showing the result of compliance checking for the functional area ordered by any criteria.

Enter the data for functional areas in the category <Business Roles>\<Basic configuration data>\<functional areas>. To do this you have to log onto the system with a role based authentication module in the application role <business roles>\<Administrators>. You can also edit functional areas in Manager. Enter a name and detailed description for the functional area. Specify a parent functional

area if you want to organize functional area in a hierarchy. You can specify how many rule violations are permitted in a functional area for check compliance rules.

Functional Area Input



Application Roles

Attestor

In the Identity Manager, you can assign employees that can be used as attestors for attestation instances to every role. To do this, assign an application role <Attestor> to the general master data for a department (cost center, location, business role). Assign employees that are authorized to attest permissions, requests or other data stored in the Identity Manager to this application role. If there is no attestor assigned to a department (cost center, location, business role), the Identity Manager determines the attestor from the parent node. If still no attestor can be determined, the attestation instance is presented to the attestor from the associated role class for approval.

Edit attestors in the Manager in the category <Organizations>\<Basic configuration data>\<Attestation>\<Attestors> or <Business Roles>\Basic configuration data>\<Attestators> or in the Identity Manager in the category <Identity Manager administration>. For detailed information about application roles see section The Identity Manager Roles Model on page 61.

Role Approvers and Role Approvers (IT)

In the Identity Manager, you can assign employees that can be used as approver for IT Shop requests to every role. To do this, assign an application role <Role approver> or <Role approver (IT)> to the general master data for a department (cost center, location, business role). Assign employees that are authorized to approve requests in the IT Shop to this application role.

Edit role approvers in the Manager in the category <Organizations>\<Basic configuration data>\<Role approvers> or <Business Roles>\Basic configuration data>\<Role approvers> or in the Identity Manager in the category <Identity Manager administration>. Edit role approvers (IT) in the Manager in the category <Organizations>\<Basic configuration data>\<Role approvers (IT)> or <Business Roles>\Basic configuration data>\<Role approvers (IT)> or in the Identity Manager in the category <Identity Manager administration>. For detailed information about application roles see section The Identity Manager Roles Model on page 61.

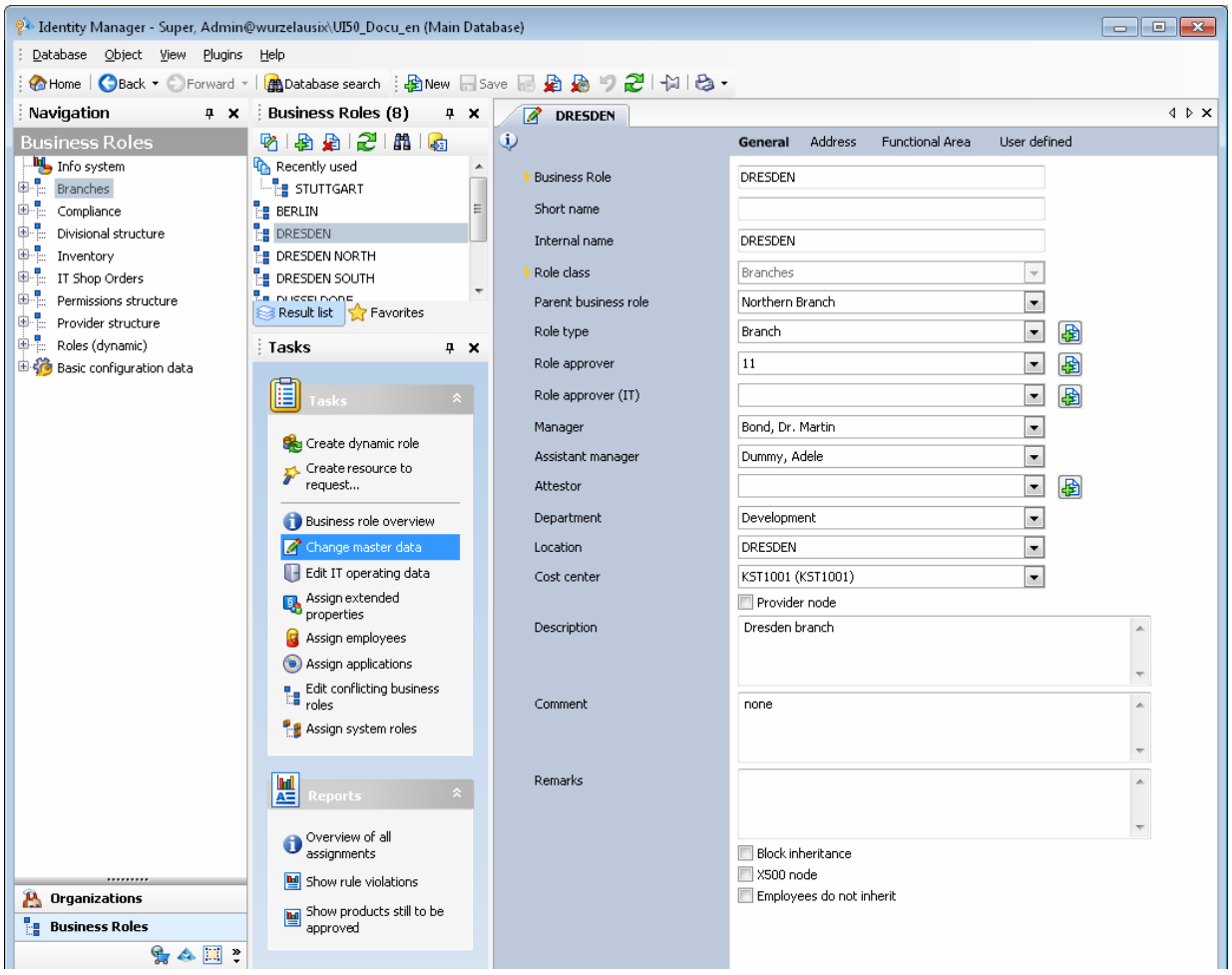
Business Roles

Modify business roles in the Identity Manager in the category <Business Roles>. To do this you have to log on to the system with a role based authentication module in the application role <Business roles>\<Administrators>". You can also edit business roles in Manager.

Business roles are grouped by role class in the navigation view. To add a new business role, select the role class that the new business role will be assigned to. The selected role class is already displayed on the master data form for the new business role.

The following master data is entered for a business role. Take care that all compulsory fields are filled.

Adding a Business Role



General Master Data

Enter an identifier, an abbreviated name and an internal name for the business role. Specify a role class. Once the business role data has been saved you can not change the role class. Select a parent business role in order to create a hierarchical role structure. Leave this input empty if the business role is at the top level of hierarchy. You have to customize parent business roles in oder to change the position of a business role within the hierarchy at a later date. Only the business roles that belong to the same role class can be selected.

Assign a role type to a business role if you want continue structuring within a hierarchy. Role types are used for displaying business roles in the user interface, for example (menu item <Role types>). If you add a level, you divide the business role up further. You need to take care that the levels also have to

be sorted hierarchically if the business roles are arranged hierarchically. You then have to specify an employee to be responsible for the business role and to assign a department, cost center or a location to the role.

With the addition of approvers, you specify the application role that employees should be taken from for authorizing decisions in an IT Shop authorization procedure. You can refer to the section Selecting an Approver on page 59 for more information.

Use the <Attestor> input field to specify the application role for determining employees authorized to make approvals in an approval instance. Read the section Attestation Approval Procedures on page 475 for more information.

If a business role has the option <End of inheritance> attached, the inheritance of company resources is discontinued. You can read more about the effects of this option in the section Discontinuing Inheritance on page 75. The option <Provider node> identifies how a provider client is used in provider mode. You can take further information from the chapter Provider Mode in the Identity Manager on page 389. The option <X500 nodes> labels a business role for export to an X500 schema.

Address

Enter the address and telephone contact data for the business role.

Functional Area

Here, you can enter values to classify the business roles, which analyses the risk of a business role with respect to identity audit. For this you need to allocate a functional area with profit and turnover for the area, the risk index for rule violations, the permitted number of rule violations and a transparency index for the area.

User Defined Master Data

This tab is used to gather further company specific information for a business role. With Designer, you can customize the display names, formats and formatting rules for the input fields (by default <Spare field no. 01> to <Spare field no. 10> and <Spare date no. 01> to <Spare date no. 03>) to meet your requirements.

Reports about Business Roles

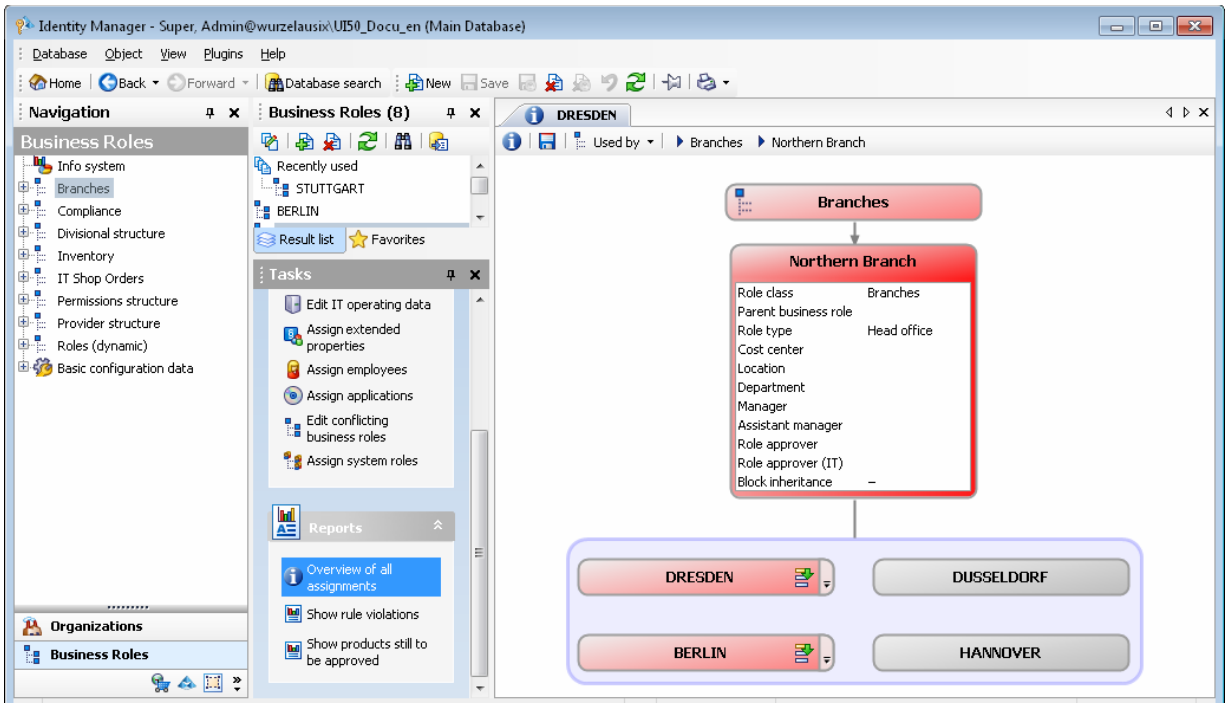
The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for business roles.

Overview of all Assignments

This report shows all employees that are members of the chosen business role. The report shows which roles of a role class the employee belongs to. Employees that are not members of any role are not ta-

ken into account. What you get is an organigram of the different role classes for the selected business role.

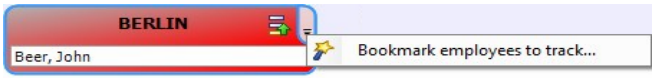
Report „Overview of all Assignments" for a Business Role



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that violate the role and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

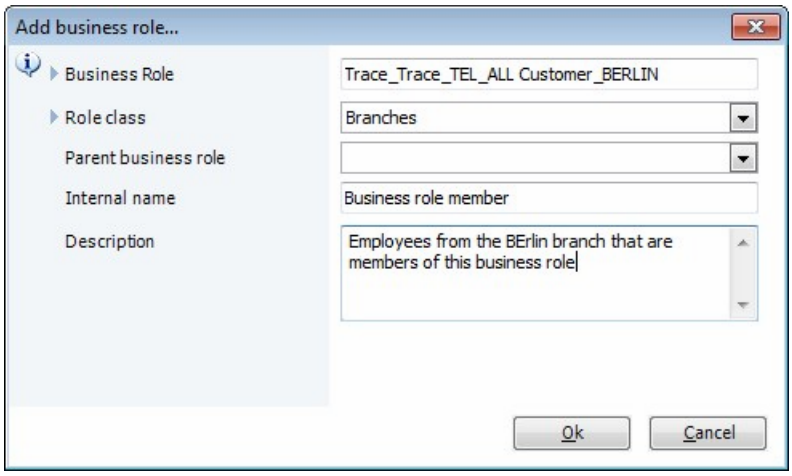
Bookmark Employee for Tracking



To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

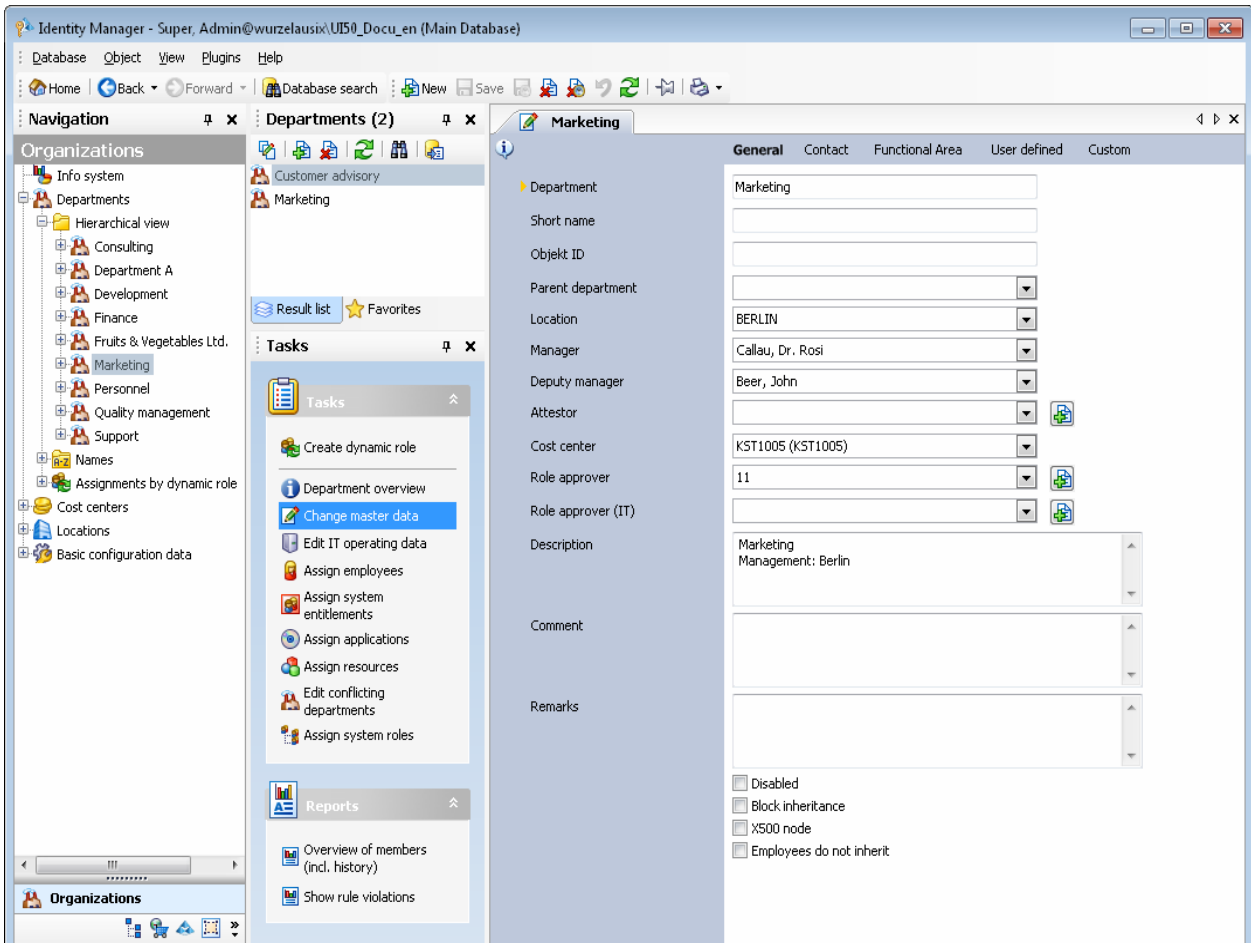
- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Departments

Modify departments in Identity Manager in the category <Organizations>. To do this you have to log on to the system with a role based authentication module from the application role <Organizations>\<Administrators>. You can also edit departments in Manager. Enter the data described in the following for a department. Please ensure that you have entered all the compulsory fields.

Setting Up a Department



General Master Data

Enter the department identifier and abbreviated name. In order to display departments hierarchically, select a parent department. Leave this entry empty if the department forms the root of the department structure. In order to change the positions of a department in the hierarchy later, you need to customize the parent departments accordingly. You also need to specify the department manager and deputy manager. Assign a department and a cost center to the department. You can also specify a default printer for the department.

With the addition of approvers, you specify the application role that employees should be taken from for authorizing decisions in an IT Shop authorization procedure. You can refer to the section Selecting an Approver on page 59 for more information.

Use the <Attestor> input field to specify the application role for detemining employees authorized to make approvals in an approval instance. Read the section Attestation Approval Procedures on page 475 for more information.

Company resource inheritance is always ”top-down“ within a department structure. If a department has the option <End of inheritance> attached, inheritance is discontinued. You can read more about the effects of this option in the section Discontinuing Inheritance on page 75. The option <X500 nodes> labels a department for export to an X500 schema.

Use the options <Employees do not inherit> to temporarily prevent employees inheriting company resources from the department. If these options are set, employees in this department do not inherit. This means that you can make all the necessary assignments to the department. Company resources can only be inherited when the options are disabled, for example, after a sharing processing has been run.

Contact

Give the contact details for the department such as email addresses, opening hours, address, telephone hours and business hours.

You can enter the auditor, audit date and your comment about the last check of the role data as audit data.

Functional Area

Here, you can enter values to classify the business roles, which analyses the risk of a business role with respect to identity audit. For this you need to allocate a functional area with profit and turnover for the area, the risk index for rule violations, the permitted number of rule violations and a transparency index for the area.

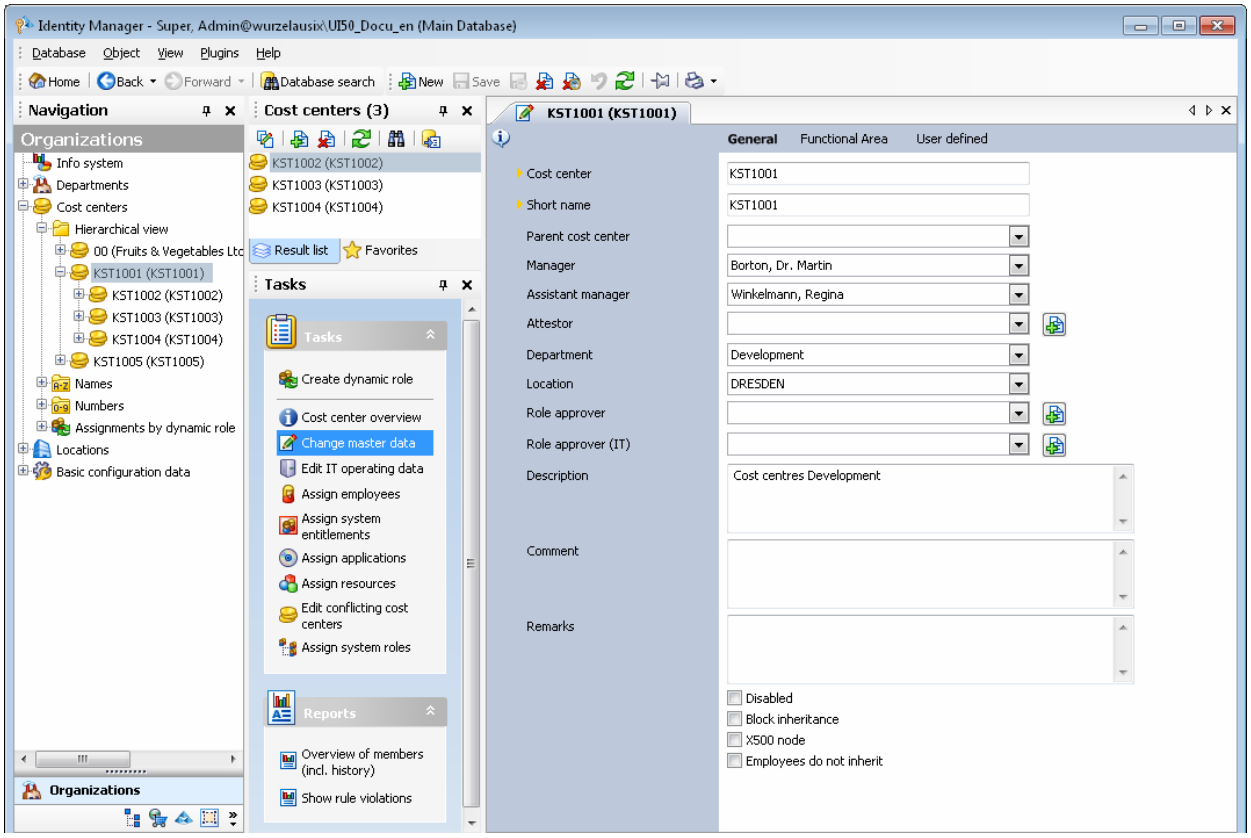
User Defined

This tab is used to gather further company specific information for a department. With Designer, you can customize the display names, formats and formatting rules for the input fields (by default <Spare field no. 01> to <Spare field no. 10> and <Spare date no. 01> to <Spare date no. 03>) to meet your requirements.

Cost Centers

Modify cost centers in Identity Manager in the category <Organizations>. To do this you have to log on to the system with a role based authentication module in the application role <Business roles>\<Administrators>. You can also edit cost centers in Manager. Enter the data described in the following for a cost center. Ensure that you have entered all the compulsory fields.

Setting Up a Cost Center



General Master Data

Enter the cost center identifier and abbreviated name. In order to display cost centers hierarchically, select a parent cost center. Leave this entry empty if the cost center forms the root of the cost center hierarchy. In order to change the positions of a cost center in the hierarchy later, you need to customize the parent cost center accordingly. You also need to specify the cost center manager. Assign a department and a location to the cost center. You may disable a cost center if it is no longer in use.

With the addition of approvers, you specify the application role that employees should be taken from for authorizing decisions in an IT Shop authorization procedure. You can refer to the section Selecting an Approver on page 59 for more information.

Use the <Attestor> input field to specify the application role for detemining employees authorized to make approvals in an approval instance. Read the section Attestation Approval Procedures on page 475 for more information.

Company resource inheritance is always ”top-down“ within a cost center structure. If a cost center has the option <End of inheritance> attached, inheritance is discontinued. You can read more about the effects of this option in the section Discontinuing Inheritance on page 75. The option <X500 nodes> labels a cost center for export to an X500 schema.

Use the options <Employees do not inherit> to temporarily prevent employees, hardware or workdesks inheriting company resources from the cost center. If these options are set, employees in this cost center do not inherit. This means that you can make all the necessary assignments to the cost center. Company resources can only be inherited when the options are disabled, for example, after a sharing processing has been run.

Functional Area

Here, you can enter values to classify the business roles, which analyses the risk of a business role with respect to identity audit. For this you need to allocate a functional area with profit and turnover for the area, the risk index for rule violations, the permitted number of rule violations and a transparency index for the area.

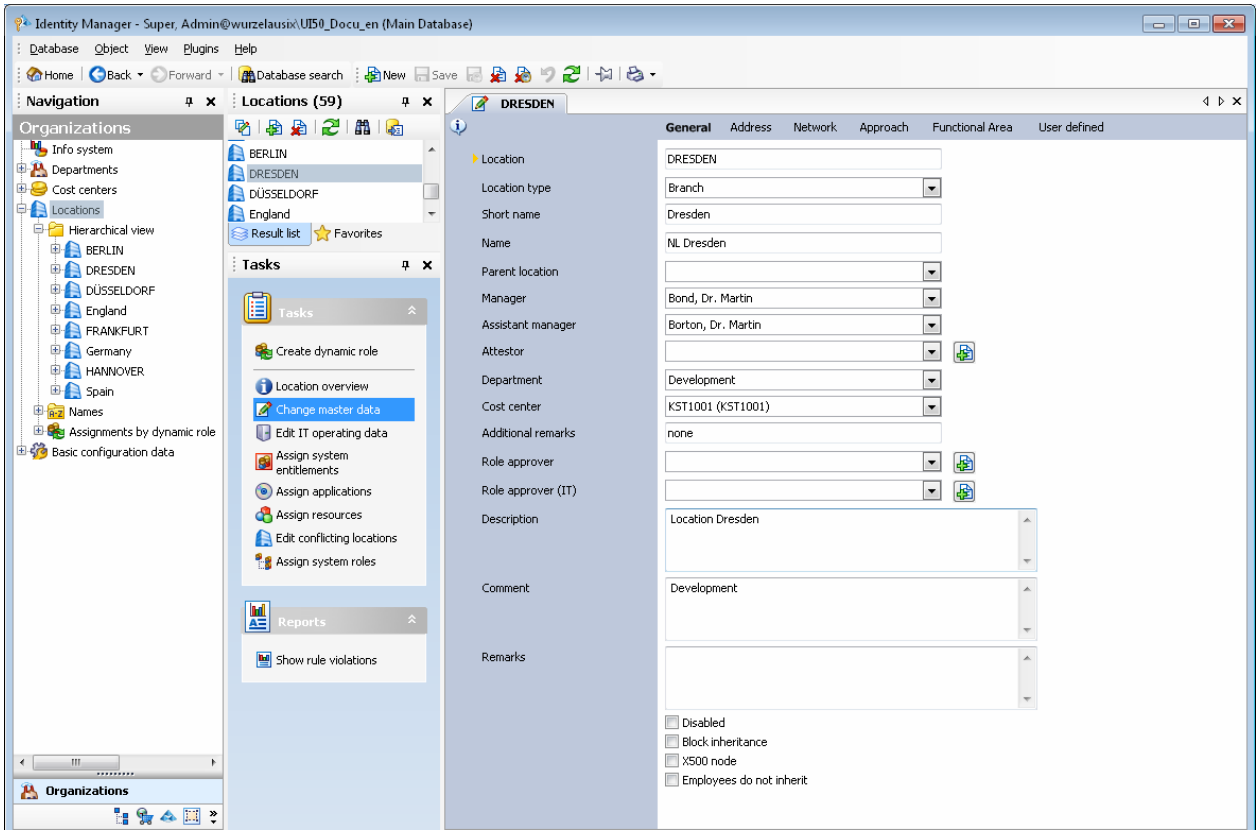
User Defined Master Data

This tab is used to gather further company specific information for a cost center. YWith Designer, you can customize the display names, formats and formatting rules for the input fields (by default <Spare field no. 01> to <Spare field no. 10> and <Spare date no. 01> to <Spare date no. 03>) to meet your requirements.

Locations

Modify locations in Identity Manager in the category <Organizations>. To do this you have to log on to the system with a role based authentication module in the application role <Business roles>\<Administrators>. You can also edit locations in Manager. Enter the data described in the following for a location. Ensure that you have entered all the compulsory fields.

Setting Up a Location



General Master Data

Enter a name for the location. You can also enter a location type, an abbreviated name and a detailed description of the location to identify it further. In order to display location hierarchically, select a parent location. Leave this entry empty if the location forms the root of the location structure. In order to change the positions of a location in the hierarchy later, you need to customize the parent location accordingly. You can also specify the location manager. Also, assign a cost center and a department to the location.

With the addition of approvers, you specify the application role that employees should be taken from for authorizing decisions in an IT Shop authorization procedure. You can refer to the section Selecting an Approver on page 59 for more information.

Use the <Attestor> input field to specify the application role for detemining employees authorized to make approvals in an approval instance. Read the section Attestation Approval Procedures on page 475 for more information.

Company resource inheritance is always ”top-down“ within a location structure. If a location has the option <End of inheritance> attached, inheritance is discontinued. You can read more about the effects of this option in the section Discontinuing Inheritance on page 75. The option <X500 nodes> labels a location for export to an X500 schema.

Use the options <Employees do not inherit> to temporarily prevent employees, hardware or workdesks inheriting company resources from the location. If these options are set, employees in this location do not inherit. This means that you can make all the necessary assignments to the location. Company resources can only be inherited when the options are disabled, for example, after a sharing processing has been run.

Address

Enter the address and telephone data required to attain the location.

Network

Store the location‘s network configuration data here.

Approach

On this tab you can enter another address and a description of the way to reach the location.

Functional Area

Here, you can enter values to classify the business roles, which analyses the risk of a business role with respect to identity audit. For this you need to allocate a functional area with profit and turnover for the area, the risk index for rule violations, the permitted number of rule violations and a transparency index for the area.

User Defined Master Data

This tab is used to gather further company specific information for a location. With Designer, you can customize the display names, formats and formatting rules for the input fields (by default <Spare field no. 01> to <Spare field no. 10> and <Spare date no. 01> to <Spare date no. 03>) to meet your requirements.

Additional Tasks for Managing Roles

After you have entered the master data for a business role, department, cost center or location, you can apply different tasks to it. You find the most important information on the overview form. There are several forms available via the task view which you can use to run the following tasks:

Some of these tasks can be only be called in the Manager. Therefore, the tool that contains the task is given as well.

Editing IT Operating Data

Tool: Identity Manager, Manager

You can enter IT operating data necessary for creating user accounts on the <Edit IT operating data> form. Read more about this in section Setting Up IT Operating Data on page 99.

Assigning Company Resources

Company resources can be inherited by assigning business roles, departments, cost centers and locations to employees objects. Indirect assignment is the default method for distributing company resources. Read the section Assigning Company Resources through Roles on page 78 for more information.

Use the following information to make company resource assignments.

TASK	TOOL
Assign system entitlements	Manager
Assign applications	Identity Manager, Manager
Assign resources	Identity Manager, Manager
Assign AD groups	Manager
Assign LDAP groups	Manager
Assign Notes groups	Manager
Assign SAP groups	Manager
Assign SAP profiles	Manager
Assign SAP roles	Manager
Assign structural profiles	Manager
Assign system roles	Identity Manager, Manager

Assigning Employees

Tools: Identity Manager, Manager

You need to assign employees to business roles, departments, cost centers or locations so that employees can inherit company resources. Refer to section Assigning Company Resources through Roles on page 78 for more information.

Assigning Extended Properties

Tools: Identity Manager, Manager

You can assign extended properties to business roles. Extended properties are meta objects that cannot be directly mapped in the Identity Manager, for example, operating codes, costing codes or cost accounting areas. These extended properties are implemented in compliance rule testing. You can find more informationin the section Setting Up Extended Properties on page 424.

Edit Dynamic Roles

Tools: Identity Manager, Manager

Use the task <Edit dynamic roles> to define dynamic roles for single business roles, departments, cost centers or location. Read section Working with Dynamic Roles on page 100 for the definition and functionality of dynamic roles.

Assign Business Roles and Organizations

Tool: Manager

Use the task <Assign business roles and organizations> to map department, cost center or location relations to other roles. You can only run the task for departments, cost centers or locations.

The task has the same effect as assigning organization on the roles master data form. The assignment is entered in the respective foreign key column in the base table..

Editing Conflicting Roles

Configuration Parameters for Editing Mutually Exclusive Roles

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Structures\ExcludeStructures	Preprocessor relevant configuration parameter for controlling the model parts that specify conflicts between roles. After changing the parameters you have to compile the database. If the parameter is set, you can specify which roles are mutually exclusive.

Tools: Identity Manager, Manager

Use this task to specify which business roles, departments, cost centers or location are mutually exclusive. You may not assign these roles to the same employees. Parent nodes definitions do not have any influence on subordinate roles.

Specifying Role Relations

Configuration Parameter for Editing Role Relations

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Structures\RelatedStructures	Preprocessor relevant configuration parameter for controlling the model parts that specify relations between roles. After changing the parameters you have to compile the database. If the parameter is set, you can specify which roles are mutually exclusive.

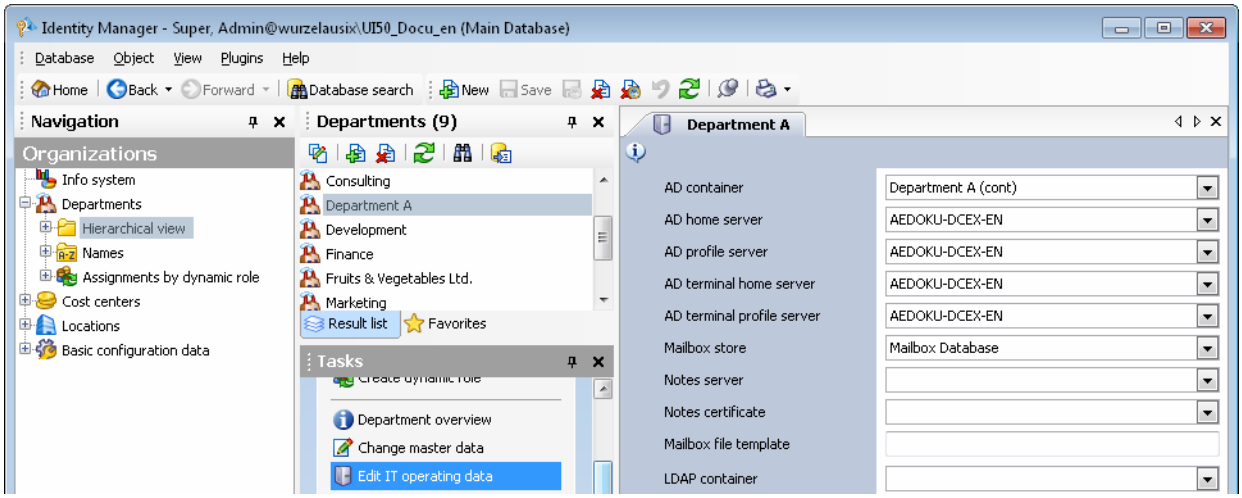
Tools: Identity Manager, Manager

Use this task to specify which relations exist between business roles, departments, cost centers and locations. This mapping is only for informative use. Parent node defintions do not provide information about role relations of subordinate roles.

Setting Up IT Operating Data

The IT operating data that automatically supplies the user accounts and IT resources (home server, profile server) to an employee, is mapped by departments, locations and cost centers and business roles. You can specify the IT operating data for role using the task <Edit IT operating data> in the Manager in the categories <Business Roles> and <Organizations>. To do this you have to log on to the system with a role based authentication module in the application role <Business roles>\<Administrators> or <Organizations>\<Administrators>. You can also edit IT operating data in Manager.

IT operating data for a Department with Target System Active Directory as Example



Permitted IT operating data is shown in the table below.

Target System IT operating data

TARGET SYSTEM	IT OPERATING DATA
Unified Namespace	Container (per target system type)
Active Directory	ADS Container
	ADS Home Server
	ADS Profile Server
	ADS Terminal Home Server
	ADS Terminal Profileserver
Microsoft Exchange	Mailbox store
LDAP	LDAP Container
Lotus Notes	Notes Server
	Notes Certificate
	Template for mail file

The IT operating data is ascertained in accordance with the company's structure and has to be customized accordingly. The method for determing the valid IT operating data is explained in the section Determining the IT Operating Data for an Employee's User Account on page 32.

Working with Dynamic Roles

Dynamic roles are used to combine objects with the same properties and to apply assignments collectively to these objects. For example company resources can be assigned dynamically to all employees in a business role in this way. It is also possible to dynamically assign a customer node in IT Shop to all the employees in a department.

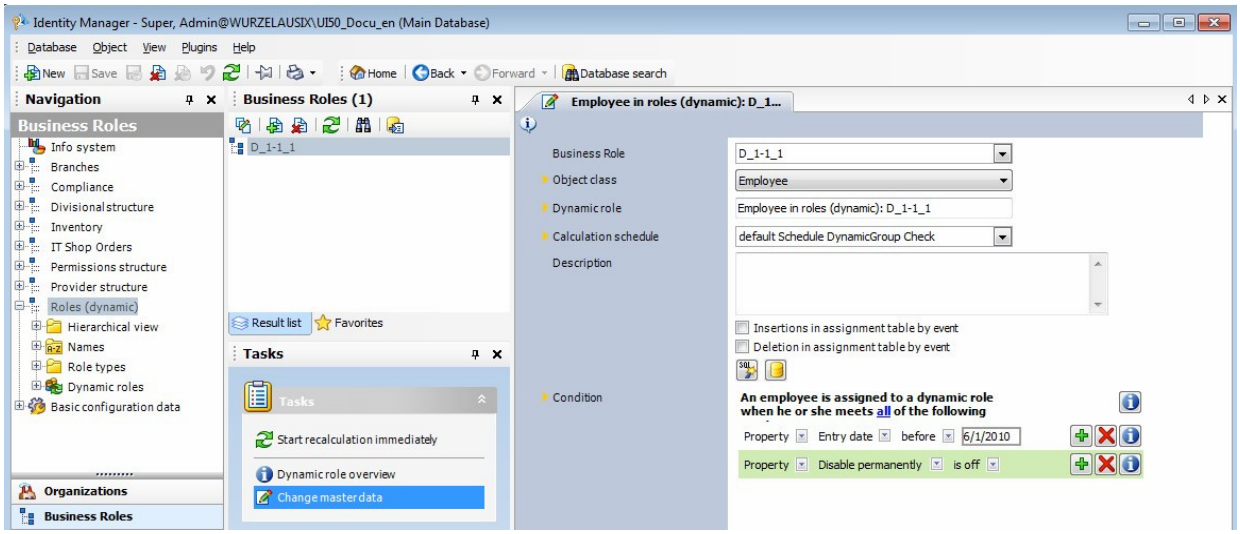
You can implement dynamic roles for business roles, departments, cost centers, locations or IT Shop customer nodes. Dynamic roles always relate to the secondary role assignment of an employee object. Therefore secondary company resource assignments must be permitted. If necessary, further configuration settings need to be made. Refer to the section Possible Company Resource Assignments via Roles on page 79 for more information.

Setting Up Dynamic Roles

Edit dynamic roles in Identity Manager in the categories <Business Roles> and <Organizations>. To do this you have to log on to the system with a role based authentication module in the application role <Business role>\<Administrators> or <Organizations>\<Administrators>". You can also edit dynamic roles in Manager. You can set up roles for dynamically assigning customers in the IT Shop in the category <IT Shop>. To do this, login with the application role <IT Shop>\>Administrators>.

To create a new dynamic role, select a role in the navigation view and run the task <Create a dynamic role>. To edit an existing dynamic role, select the dynamic role by double-clicking on it in the role overview form.

Dynamic Role Data



Enter the following data for a dynamic role:

- The object class that the dynamic role is valid for. "Employee" is a permissible object class.

- The business role that the dynamic roles is refers to.
  This input is preset with the selected business role. If the objects meet the dynamic role condition, they become members in this role.

The combination of an object class (employee) together with a business role has to be unique. It is not possible, therefore, to allow two dynamic roles from the same object class to refer to one business role.

- The identifier that the role can be selected by
- Calculation schedule
  Scheduled task triggered by cyclical recalculation of the dynamic role. Read section Setting Up a Scheduled Task to Calculate Dynamic Roles on page 103 for more information.
- A detailed description
- Input whether inserts/deletes should take place per event.
  These options determine how data sets are inserted and deleted in assignment tables. Refer to section Calculating Role Memberships on page 102 for more information.
- The condition that describes membership in a dynamic role.
  The condition is used to define which object class object will become a member of a dynamic role and therefore any associated business role, department, cost center or location-. The condition is defined as a valid Where clause for a database query and has to relate to the selected object class. You can enter the condition directly as an SQL statement. Alternatively, you can enter conditions for employee objects with the filter designer. Read section Rule Editor for Entering Rule Conditions on page 172 to learn about using the filter designer.

You must enter a condition for a dynamic role! If the condition includes large numbers of objects, the subsequent number of assignments taking place can result in a heavy load on the DBScheduler and therefore also on the database server.

The DBScheduler cannot interpret the comment characters '--', '//' or '%' within a condition. The calculation will be aborted.
Use the '/*' and '*/' strings to enclose comments!

You can use the additional task <Test condition> to test which objects meet the given condition before you save it.

Calculating Role Memberships

Configuration Parameters for Calculating Dynamic Roles

CONFIGURATIONS PARAMETER	MEANING
QER\Structures\DynamicGroupCheck	This configuration parameter controls the generation of calculation tasks for dynamic roles..
QER\Structures\DynamicGroupCheck\CalculateImmediatelyPerson	This configuration parameter specifies the intervals at which recalculation tasks for dynamic roles with object type ”Person“ should be set. If the parameter is set, modifications to employees or employee level objects a calculation task is for the DBScheduler is started immediately. If the parameter is not set, the calcuation tasks are started the next time the scheduled task is executed.

If a role is assigned to a dynamic role, employees are only assigned via dynamic roles. Manual assignments to the roles are reverted by the Identity Manager assuming the objects do not fulfill the conditions for the dynamic role. Modifications to the assignment are not calculated until the next scheduled task is run.

In order to calculate role memberships, the Identity Manager tests every dynamic role to ensure that:

- There is at least one object that satifies the condition but is not assigned to the role.
- There is at least one object that does not satisfy the the condition but is assigned to the role

If one of the conditions is fulfilled, a request to add or delete memberships is sent to the DBScheduler. When the dynamic roles are tested, employee objects that are marked for deletion (vi_consistent = ’D’) are:

- not added to roles via dynamic roles even if the miscellaneous condition is fulfilled.
- removed from the role even if the miscellaneous condition should be fulfilled.

Depending on the setting of the configuration parameter, the membership recalculation request is set up by:

- Cyclical checking using a scheduled task“
  All dynamic role memberships are checked and recalculation requests are sent to the DBScheduler if necessary. Checks are made at predefined intervals. The scheduled task start interval is initially set to the same value as the DBScheduler. You can set the start interval in the scheduled task.
- Immediately an object has changed
  Memberships are immediately checked by the DBScheduler and changed is necessary when object properties are changed. If a larger number of objects are effected, they are calculated by the scheduled task and not processed individually.

Manual assignments of employeesto roles are only tested and recalculated during a scheduled task.

The dynamic role definition also has the following two options:

- Insert assignment table by event
- Delete assignment table by event

If these options are not set for dynamic roles, the affected data sets are inserted or deleted directly in the assignment tables by the DBScheduler. If the options are set, processes for the process component

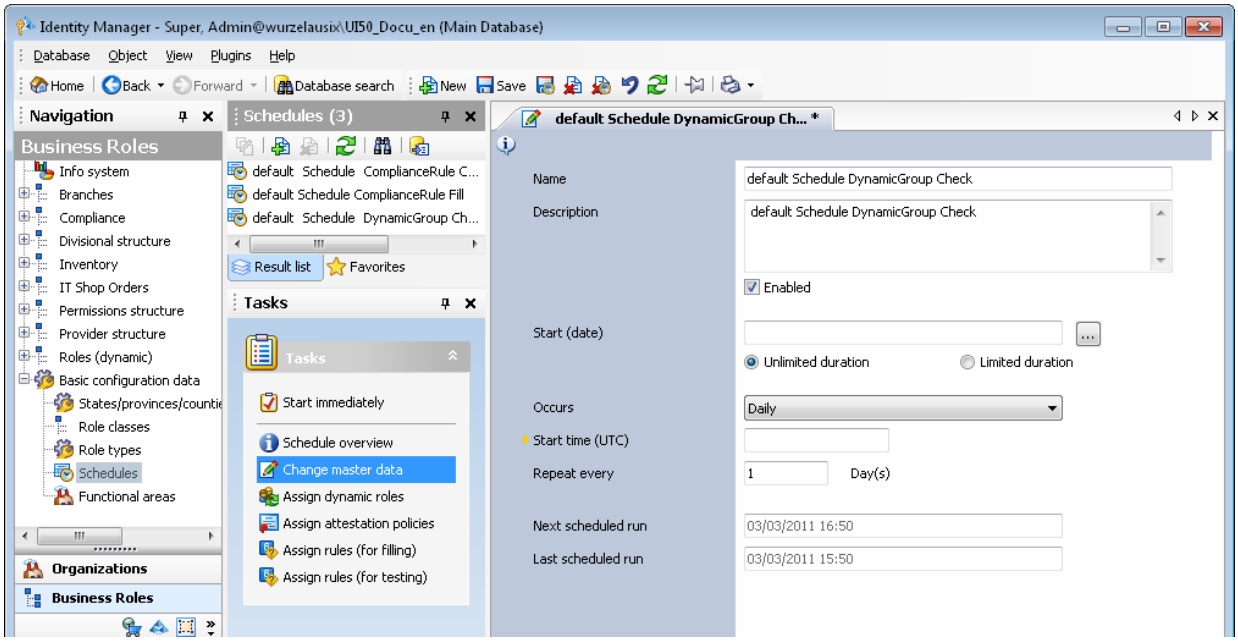
HandleObject are set up in the Job queue that carry out the respective operations. This makes it possible to link specific processes to the assignment tables' insert and delete events. This behaviour has to implemented on a custom basis.

Setting Up a Scheduled Task to Calculate Dynamic Roles

Use scheduled tasks to calculate dynamic groups on a cyclical basis. The task "default Schedule DynamicGroup Check" is already defined in the standard version of the Identity Manager, which you can modify to suit your requirements. You can also set up new scheduled tasks.

Edit scheduled tasks for dynamic roles in Identity Manager in the category <Business Roles>\<Basic configuration data>\<Schedules>. To do this you have to log on to the system with a role based authentication module in the application role <Business role>\<Administrators> or <Organizations>\<Administrators>. You can also edit role classes in Manager.

Process Schedules for Calculating Dynamic Roles



The general properties described in the following are expected for a scheduled task:

- Task ID
- Detailed description of the schedule task
- Enabling the task

Configure the execution times with the following settings:

- Valid time period
  Use the options <Unlimited duration> and <Limited duration> and the input fields <Start (date)> and <End (date)> to specify the valid time period for the scheduled task. Enter the first day that the task should be performed on and the last time it should be run.

- Start date for the task
  Specify the interval for executing the task. The start time is calculated from the frequency of the interval (<Repeat every>) and the interval type. Permitted interval types (<Occurs>) are minute, hous, day, week, month and yearly. In cases of interval types week, month, year, you need to specify the day of the week, month, year. You also have to specify a fixed start date for the interval types day, week, month and year. The time is specified in UTC.

- Start information
  The start information contains the time that the scheduled task was last run (<Last planned run>) and the time at which it will be run next (<Next planned run>). The time of the next run is calculated from the start time specified. The Identity Manager provides the start information in the time zone of the client where the program was started.

Run the task <Assign dynamic roles> to assign the scheduled task to a dynamic role.

Calculating Execution Times

The scheduled task ”vi_PayLoadSchedule“ checks the tasks and their start times regular intervals.

When the database scheduler is run, all tasks are found that are within the valid time period and are enabled. From this set, all tasks are generated that have reached or exceeded their time of execution. Following on, the time for the next run is calculated and entered in the start information in the scheduled task.

For tasks with interval types minute and hour, the next schedule start time is calculated from the current time and the rate of execution. Because of this, the time may be displaced by a matter of seconds.

These displacements may cause scheduled tasks to hold exactly to the execution times given in the interval rates.

The next execution time for tasks with the interval types day, week, month and year are calculted from the given sub-interval and the start time. The next time for executing the task always agrees exactly with the start time.

Scheduled tasks that have the sub-interval ”31“ as interval type, month are run on the ”31st of the month“. The task is, therefore, only run in months with 31 days. The same is true of the interval type year and the sub-interval ”336“.

The execution times for scheduled tasks that have been newly set up are empty. The last and next execution times for new tasks are calculated from the following two runs of the Jobscheduler. The execution of these tasks does not take place until the calculated point in time is reached.

5

Resource Administration

- Introduction
- Resources
- System Roles
- System Entitlements, Groups, Applications

Introduction

The Identity Manager not only offers the possibility to manage IT resources but also non-IT resources such as mobile telephones, desks, company cars and keys i.e, everything that is necessary to create an efficient working environment for an employee.

In order to assign user accounts automatically to employees during working hours, special resources are defined in the Identity Manager. These user account resources can be created for any area of the target system in use, for example, the different AD domains of an Active Directory environment. Creating the user account resources is described in the respective chapter for the target system.

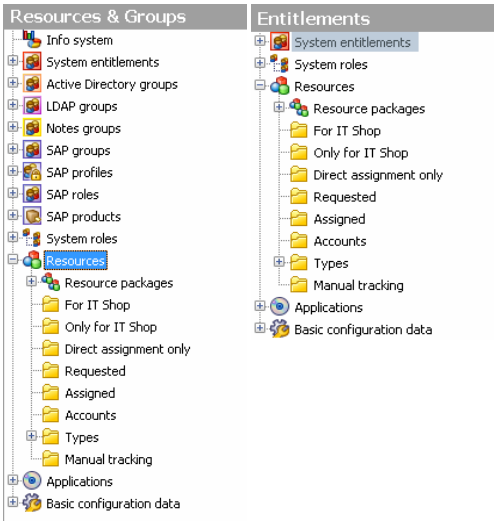
In addition to this, any number of company resources can grouped together in packages, known as ”system roles“ in the Identity Manager. If these system roles are assigned to employees, those employees inherit all the company resources that are assigned to the system role. This can be system entitlements, applications or non-IT resources, for example.

Resources

Resources can be directly assigned to an employee or via classification in roles. Similarly, resources can be requested for an employee via the IT Shop. After a resource has been assigned, further manual editing may be necessary.

You can edit resources in the Manager in the category <Resources & Groups>\<Resources>. You can also edit resources in the Identity Manager in the category <Entitlements>\<Resources>. To do this, login with a role based authentication module from the application role <IT Shop>\<Administrators>.

Displaying Resources in Manager and Identity Manager



Base Data for Resources

Resource Types

Resources require a resource type. The resource type is used to specify further post-processing steps for a resource request or a resource assignment. Firstly, define the necessary resource types in the ca-

tegory <Resources & Groups>\<Basic configuration data>\<Resource types>. Enter a name and a detailed description for the resource type.

Processing Status

After a resource has been assigned, further manual processing may be necessary. You can define processing statuses in the Identity Manager that reflect the status of each manual processing step.

Example:

An employee requests a mobile phone through the IT Shop. This request is authorized by the person in charge of the employee's cost center. The following steps could be necessary:

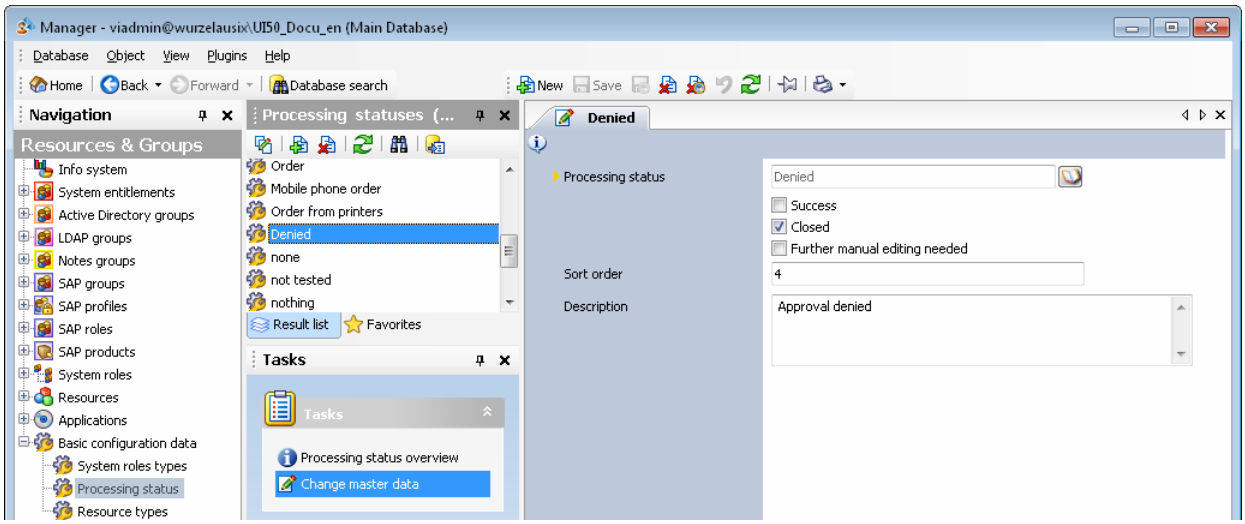
- Initiate phone request at the dealers
- Check delivery
- Activate the resource in asset accounting
- Deliver phone to employee

Once a processing step has been completed the processing status for the assigned resource should be updated. Employees can use this to keep up-to-date with the progress of their requests.

Manual post-processing of resource requests is not part of the standard Identity Manager installation. Implement a custom solution for the required functionality!

You can specify the individual steps for manual tracking in the category <Resources & Groups>\<Basic configuration data>\<Processing status>.

Setting Up the Processing Status



Enter the following information into processing status:

- Description of the processing status

- Status attributes
  Use the options <Success>, <Closed> and <Manual post-processing> to distinguish between processing statuses of different manual post-processing steps.

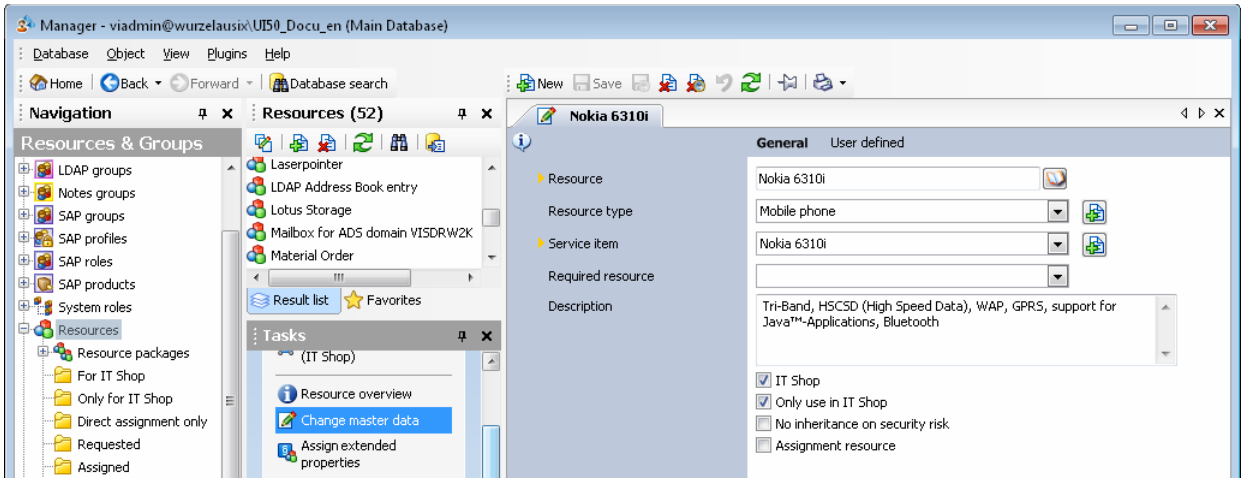
- Sequence
  Use the sequence to specify which status a resource request should have initially once the request has been successfully assigned. Other processing statuses can only be set once certain manual post-processing steps have been handled.

You can use user defined columns, for example, to link processing statuses to resources (<Spare field No. 1> to <Spare field No. 10>). For more information, see section Editing Resources on page 108.

Editing Resources

You can enter resources in the category <Resources & Groups>\<Resources>.

Resource Data Entry



The following data is required for a resource:

- The name and detailed description of the resource

- The resource type

- Service item
  You can assign an <service item> to a resource or add a new one. This way the resource booked internally.

- Required resource
  Here you define dependencies between resources. Wenn this resource is requested or assigned, the required resource is automatically requested or assigned with it.

- Data for use in the IT Shop
  If a resource can be requested over the IT Shop, select the option <IT Shop> (see Chapter Setting Up an IT Shop Solution on page 15). This resource can then be requested by an employee from the IT Shop and is allocated by a defined approval policy. However, you are still able to assign the resource directly to an employee and roles. To disallow the assignment, you need to set the option <Only use in IT Shop>. In this case, the resource can only be requested over the IT Shop.

- No inheritance on security risk
  Resources that are labeled with this option cannot be inherited by employees that are classified as a security risk. Read the section Employee Master Data on page 47 for more information.

- Assignment resource
  This resource is used to assign permissions using the IT Shop. Assign a service item to the IT Shop so that assignment resources can be requested through the IT Shop and set the option <IT Shop>. For more information about assignment requests refer to section Assignment Requests and Delegating on page 50 in the IT Shop Manual.

- Keeps requested assignment resource
  If this option is enabled, assignment requests remain even when the requester is removed from the customer node of the associated shop. If the requester is also the recipient of the request (such as requesting membership in a business role for the requester) the assignment is canceled anyway.
  This option is only visible if the option <Assignment resource> is enabled. The option can only be edited as long as there is a request has not been assigned with this assignment resource.

Use Defined Master Data for Resources

The tab is provided for entering additional custom data for resources. With the Designer, you can customize display names, formats and templates for the input fields (by default <Spare field no. 1> to <Spare field nr. 10>) to suit your needs.

Resource Packages

You can put individual resources together into resource packages, which simplifies assigning resources to employees and company structures. Employees can obtain resource packages directly or by inheriting them over company structures. It is also possible to request resource packages through the IT Shop. Resources where the option <Only for use in IT Shop> is enabled can only be assigned to resource packages that also have this option set.

You can setup resource packages in the category <Resources & Groups>\<Resources>\<Resource packages>. Resources packages are system roles with the system role type ”Resource package“. Resources can also be added to system roles that are not resource packages. You can read about creating system roles in the section System Roles on page 114.

The valid inheritance mechanism and calculating resource package assignments by the DBScheduler are described in detail in the Configuration Manual in section System Role Inheritance on page 283.

Additional Tasks for Managing Resources

After you have entered resource and resource package master data, you can apply different tasks to them. You can see the most important information about a resource or a resource package on the overview form. The task view contains different forms with which you can run the following tasks.

Assign System Roles

A resource can be added to different system roles. A system role that is only contains resources can be labeled with the system role type ”Resource package“. You can find other information about resource packages in section Resource Packages on page 109. Resources can also be added to system roles that are not resource packages.

Assign Business Roles and Organizations

Resources can be inherited by employees belonging to these roles via assignment to business roles, departments,cost centers and locations. This type of indirect assignment is the standard method of distributing resources to employees. Use the task <Assign business roles and organizations> to assign individual roles.

Assign to Employees

In order to react quickly to special requests, you can also assign resources and resource packages to employees with the form <Assign to Employees>. The valid inheritance mechanism and calculation of resource assignments by the DBScheduler are described in section Inheriting Resources on page 282 in the Configuration Manual.

Add Resources to the IT Shop

Once a resource or a resource package has been assigned to an IT Shop shelf, it can be requested by the shop customers. There are other prerequisites requirements to make a resource or a resource package requestable. You will find further information about this in the section Requestable Products on page 33. Use the task <Remove from all shelves (IT Shop)> to remove a resource or resource package from the IT Shop.

Assign Extended Properties to Resources

Extended properties are meta objects for which there is no direct mapping, such as accounting codes, controlling areas or cost center areas, in the Identity Manager data model. These extended properties are used to check rule conformity. For more information see section Setting Up Extended Properties on page 424.

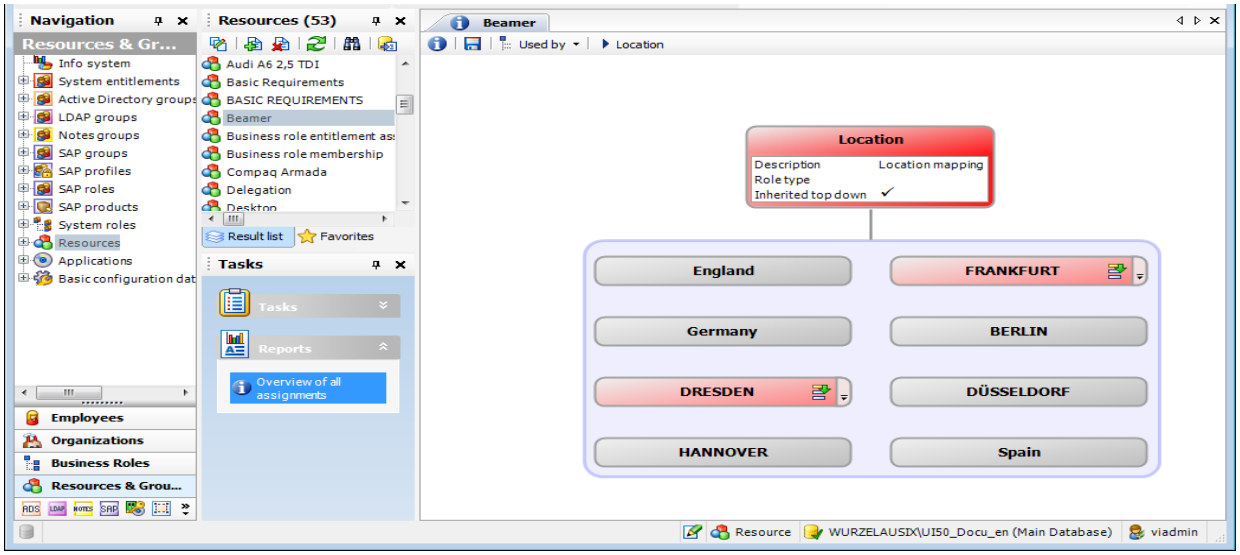
Reports about Resources

The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for resources.

Overview of all Assignments

This report shows all employees that are members of the chosen resource. The report shows which roles of a role classe the employee belongs to. Employees that are not members of any role are not taken into account. What you get is an organigram of the different role classes for the selected resource.

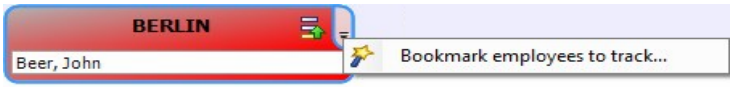
Report "Overview of all Assignments" for a Resource



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that violate the role and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

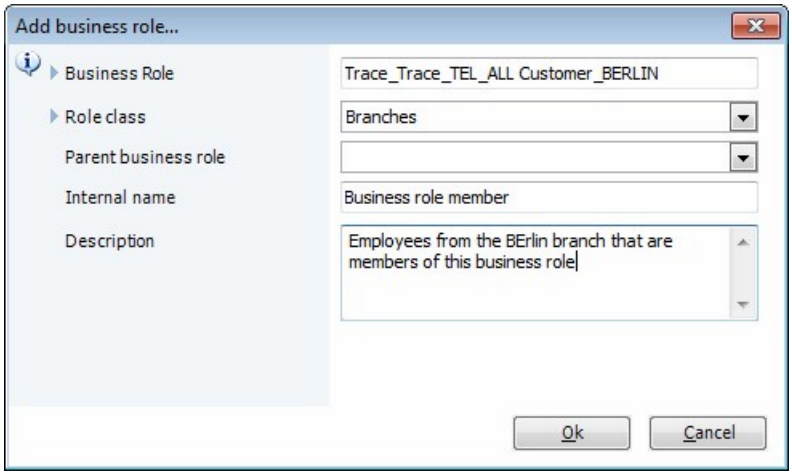
Bookmark Employee for Tracking



To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

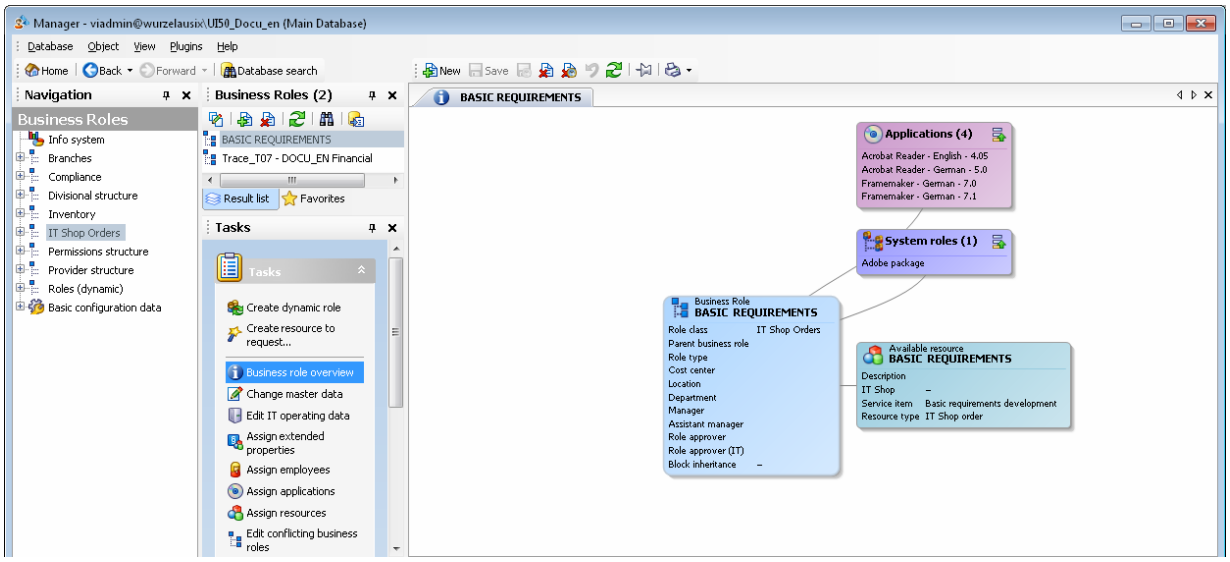
Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Mapping a Business Role to a Resource

Company resources such as applications, group membership and non-IT resources, that are usualy requested and cancelled together, can be setup as a group in a business role. The business role is based on a resource that is represented as an article and can be requested in the IT Shop.

To do this, you add a business role and assign the target systems groups and applications to it, for example.

Setting Up a Business Role to Create Resources



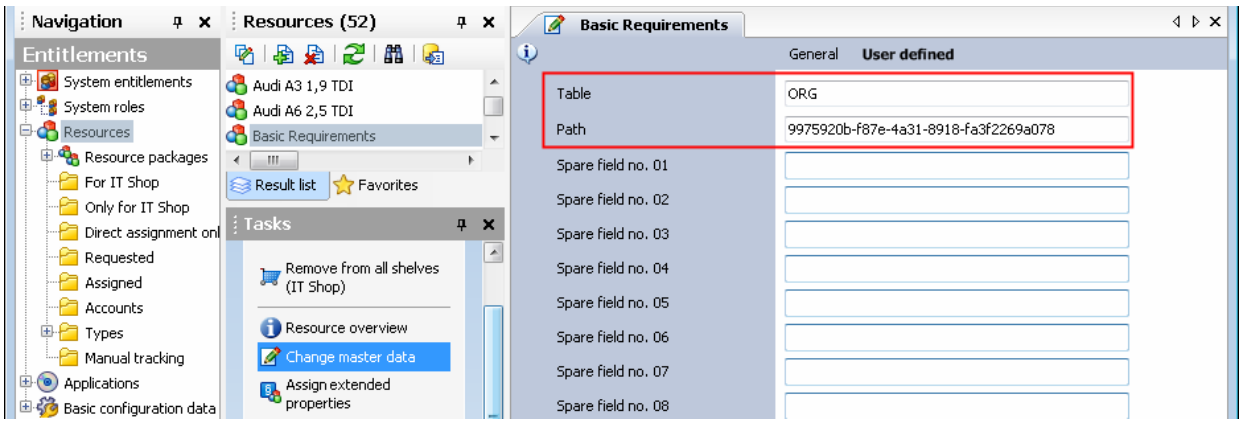
Next, add a resource that is internally linked to the business role. Use the task <Create resource to request..> for this. It starts a wizard that helps you through entering the necessary data for creating an requestable resource.

Now assign this resource to a shelf within the IT Shop. It can then be requested as an product by IT Shop customers via the IT Shop. If the IT Shop authorization process approves the request, the employee becomes a member of the business role and inherits Active Directory and Lotus Notes groups and applications through the current inheritance mechanism. If the request is cancelled or the resource is disabled, the business role membership is revoked and the assignment is removed.

The Process in Practice:

Database tables and columns are used in part in the following description. Execution of the task <Create resource to request...> on a business role causes a entry to be added to the table ”Resource“ with the attributes ”ConnectionTable“ and ”ConnectionPath“. These attributes are treated internally as user defined attributes. For each task the table ”Org“ is entered in the column ”ConnectionTable“, the column ”ConnectionPath“ contains the UID of the business role.

Resource created by Task within a Business Role



You have already specified the options, such as the <IT Shop> option and aservice item, for requesting the resource via the IT Shop with the wizard.

If an employee requests the resource as an article in the IT Shop, a entry in the table ”PersonWantsOrg“ is created. If the request is approved, it results in an entry in the table ”PersonHasRessourceTotal“ being made over the current inheritance mechanism.

As a reaction to the entry in the table ”PersonHasRessourceTotal“ a new entry is created in the table ”PersonInOrg“ by a process using the information from ”ConnectionTable“ and ”ConnectionPath“. Thus the employee is placed in the business role.

Example process:

Basic object:	PersonHasRessourceTotal
Event:	Insert
Process:	VI_Ressource_Insert PERSONINORG
Generating Condition:	Len($FK(UID_ressource),Ressource.connectionpath$) > 0 And UCase ($FK(UID_Ressource),Resource.Connectiontable$) = "Org"

with

Process:	Insert in PersonInOrg
Task:	EXECUTE SQL
Parameter: SQLSTMT	"exec viInsertForHandleObject 'Insert', 'PersonInOrg', '', 'UID_Person', '" & UID_Person & "', 'UID_Org','" & $FK(UID_Ressource),Resource.Connectionpath$ & "'"

The entry is removed from the table ”PersonHasRessourceTotal“ when the request is cancelled or the resource is deactivated. The corresponding entry in the table ”PersonInOrg“ needs to be deleted by running a process. This information is given by the attributes ”ConnectionTable“ and ”ConnectionPath“.

System Roles

System roles make it easier to assign company resources that are frequently required or rather that are always assigned together. For example, new employees in the finance department should be provided, by default, with certain system entitlements for Active Directory and for SAP. In order to avoid a lot of separate assignments, group these company resources into a package and assign this to the new employee. The packages are refered to as system role in the Identity Manager.

You can group together arbitrary company resources into packages. You can assign these system roles to employees or roles or you can request them through the IT Shop. The valid inheritance mechanism and calculation of system roles by the DBScheduler are described in detail in the Configuration Manual in section System Role Inheritance on page 283. System roles are, for example, SAP products or application packages. You can also, however, group together other company resources into system roles, such as AD groups or system entitlements. You can structure system roles by assigning other system roles to them.

Employees inherit exactly those company resource that can be inherited from the system role.
Example:

A system role contain an Active Directory group and an SAP role. An employee only has one Active Directory user account. If the system role is assigned to the employee, the Active Directory group is inherited by the Active Directory user account. The SAP role is not inherited. If this employee obtains an SAP user account at a later date, the SAP role is inherited by the SAP user account.

System Role Types

System role types identify the type of company resources that the system role is used to grouped together. The system roles <Application package>, <Resource package> and <SAP product> are supplied as standard by the Identity Manager. In addition, you can define your own system roles types, for example, system roles that group different target systems together.

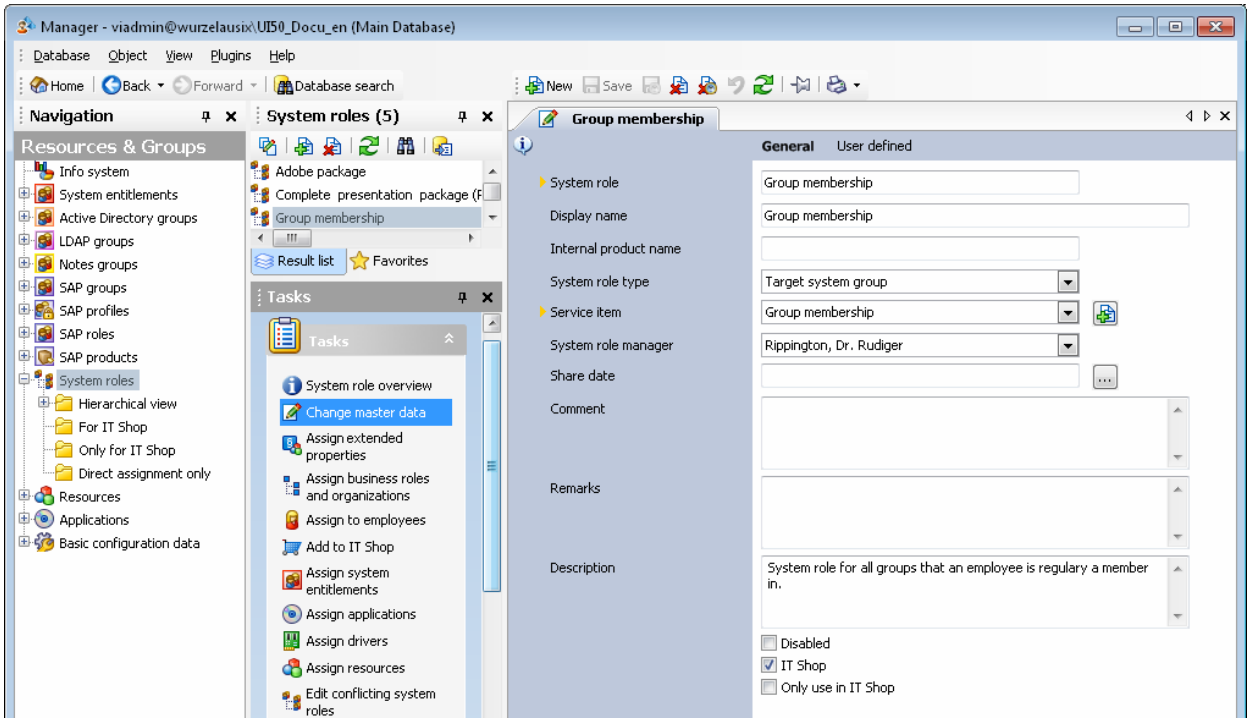
Edit system role types in Manager in the category <Resources & Groups>\<Basic configuration data>\<System role types>. You can also edit system roles types in Identity Manager in the category <Entitlements>\<Basic configuration data>\<System role types>. To to this, login with a role based authentication module from the application role <IT Shop>\<Administrators> or <Target systems>\<Target system admin>.

Editing System roles

Edit system roles in Manager in the category <Resources & Groups>\<System roles>. You can also edit system roles in Identity Manager in the category <Entitlements>\<System roles>. To do this, login with a role based authentication module from the application role <IT Shop>\<Administrators> or <Target systems>\<Managers>.

General Master Data for System Roles

System Role Setup



Enter the following data for a system role.

- Display name
  Name for displaying the system roles in the Identity Manager tools.

- System role
  Unique identifier for the system role

- Internal product name
  An additional internal name for the system role

- System role type
  Specifies which type of company resources the system role is comprised of.

- Service items
  In order to use a service item within the IT Shop, assign a service item to it or add a new service item. This allow the requested system role to be booked internally.

- System role manager
  You can assign any employee to be a system role manager.

- Share date
  Specify a date for enabling the system role. If the date is in the future, the system role is considered disabled (see option <Disabled>). If the date is already valid, the system role is enabled. Employees inherit the company resources that are assigned to the system role.

- Commentary, remark, description
  Spare text fields for your notes about the system role

- Disabled
  This option allows you to specify whether employees inherit the company resources contained in the system role.
  If the option is set, the system role can be assigned to employees and workdesm. However they cannot inherit the company resources contained in the system role.
  If the option is not set, the employees that are assigned the system role, immediately inherit company resources allocated to the system role.
  If the option is enabled at a later date, existing assignments are removed.

- Only use in IT Shop
  Label system roles that can be requested via the IT Shop (see Setting Up an IT Shop on page 18) with the option <IT Shop>. These system roles can be requested by your staff via the IT Shop and distributed using defined approval procedures. However, these system roles, can still be assigned directly to employees and roles. To prevent this from happening, set the option <Only use in IT Shop>. In this case the system roles can only be requested via the IT Shop.

There is a scheduled task ”Share system roles“ for checking the share dat. You can edit this scheduled task to meet you requirements with the Schedule Editor and start it. For more information see the section Working with the Schedule Editor on page 73 in the Process Orchestration Manual.

User Defined Master Data for System Roles

This tab is used for entering company specific data for system roles. You can modify the display names, format and templates for input fields (by default <Spare date nr. 01>, <Spare date nr. 02>, <Spare field nr. 01> to <Spare field nr. 13>, <Spare text nr. 01> to <Spare text nr. 03>) to meet your requirements.

Additional Tasks for Managing System Roles

After you have entered all the data for the system you, you can apply various tasks to them. You can find the most important information on the overview form. There are different form available on the task view that you can use to run the followig tasks.

Which tools you may use for which task is given in each case. The application role you need to use to log into the Identity Manager in order to run the task, is also given.

Assign Business Roles and Organizations

Tools: Manager, Identity Manager
Application role: <Target systems>\<Target system admin>

By assigning system roles to business roles, departments, cost centers and locations, the employees that are member of these roles can inherit the assigned system roles. This indirect assignment of system roles to employees is the default method of distributing system roles.

Assign to Employees

Tools: Manager, Identity Manager
Application role: <Target systems>\<Target system admin>

Use this task to assign system roles directly to employees. All company resources tha are assigned to the system are iherited by the employees. The company resoures are not inherited if the system role is disabled or if the share date is still in the future.

Add to IT Shop

Tools: Manager, Identity Manager
Application role: <IT Shop>\<Administrators>

A system role can be requested by shop customes when it is assigned to an IT Shop shelf. There are other prerequisites to take into account so that a system role can be requested. You can find further information in the section Requestable Products on page 33 in the IT Shop Manual. To remove a system role from the IT Shop, use the task <Remove fom all shelves (IT Shop)>.

Assign Extended Properties

Tool: Manager,Identity Manager
Application roles: <IT Shop>\<Administrators>, <Target systems>\<Target system admin>

You can assign extended properties to system roles with the system role type ”resource package“. Extended properties are meta objects for which there is no direct mapping, such as accounting codes, controlling areas or cost center areas, in the Identity Manager data model. These extended properties are used to check rule conformity. For more information see section Setting Up Extended Properties on page 424.

Assign Company Resources

Tools: see table below
Application roles: <IT Shop>\<Administrators>, <Target systems>\<Target system admin>

Assign the company resources that you want to group together into one package to the system role Employees that you assign this system role to, will inherit these company resources. Company resources labeled with the option <Only use in IT Shop>, can only be assigned to system roles that also have this option set.

Use the following tasks to asign company resouces

TASK	TOOL
Assign system entitlements	Identity Manager, Manager
Assign applications	Identity Manager, Manager
Assign resources	Identity Manager, Manager
Assign ADS groups	Manager
Assign LDAP groups	Manager
Assign Notes groups	Manager
Assign SAP groups	Manager
Assign SAP profiles	Manager
Assign SAP roles	Manager
Assign system roles	Identity Manager, Manager

Assign System roles

Tools: Manager, Identity Manager
Application roles: <IT Shop>\<Administrators>, <Target systems>\<Target system admin>

Use this task to group different system roles into one package. This enables system roles to be structured from different view points. System roles labeled with the option <Only use in IT Shop> set, can only be assigned to system roles that also have ths option set.

Edit Conflicting System Roles

Configuration Parameter for Editing Mutually Exclusive Roles

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Structures\Exclude-Structures	Preprocessor relevant configuration parameter for controlling model components for determining conflicts between roles. Aftter changing this parameter you have to recompile the database. If the parameter is set, you can specify whch roles are mutually exclusive.

Tools: Manager, Identity Manager
Application roles: <IT Shop>\<Administrators>, <Target systems>\<Target system admin>

Use this task to specify which system roles are mutually exclusive. Yo may not assign thiese roles to the same employee. Definitions for a system role are not inherited by parent or child system role. This means that conflicting system roles can be grouped together into a system role.

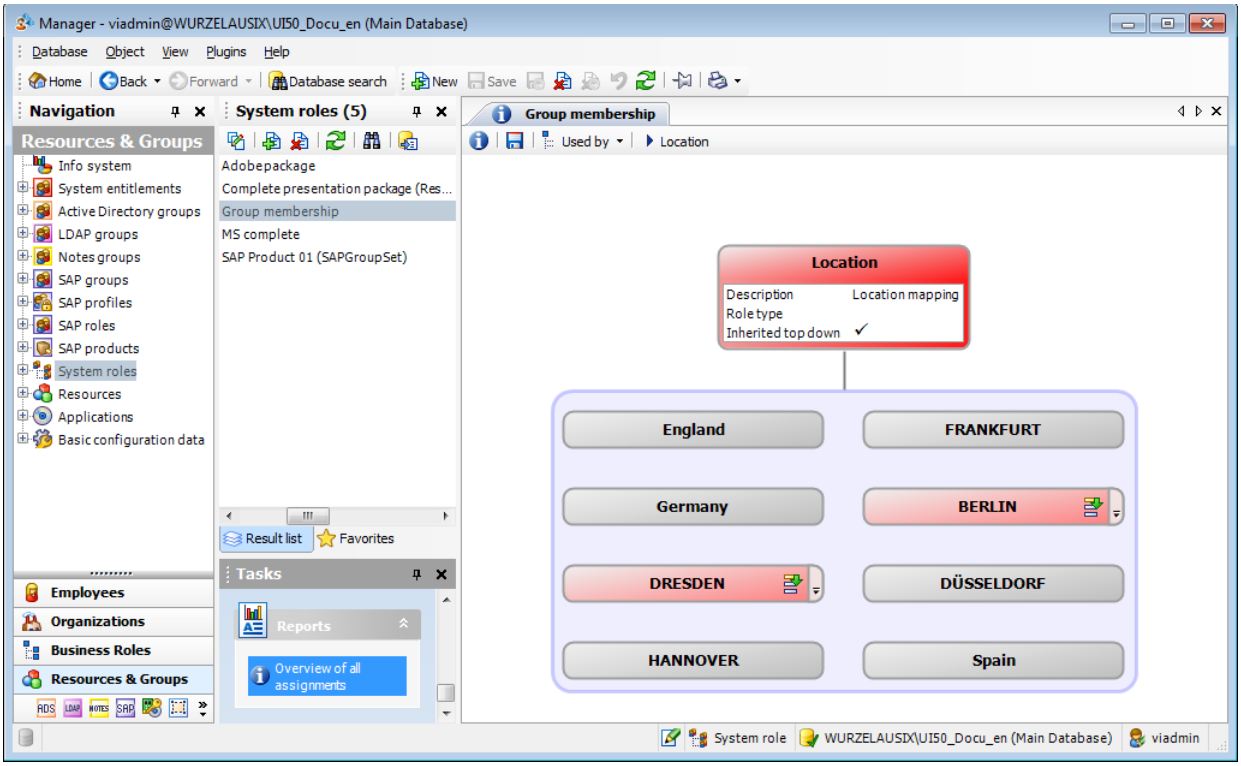
Reports about System Roles

The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for resources.

Overview of all Assignments

This report shows all employees that are assigned this system role. Both the directly assigned object and those the employee obtains through inheritance are taken into account.The report shows which roles of a role classe the employee belongs to. Employees that are not members of any role are not taken into account. What you get is an organigram of the different role classes for the selected system role.

Report "Overview of all Assignments" for a System Role



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that have the selected system role and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

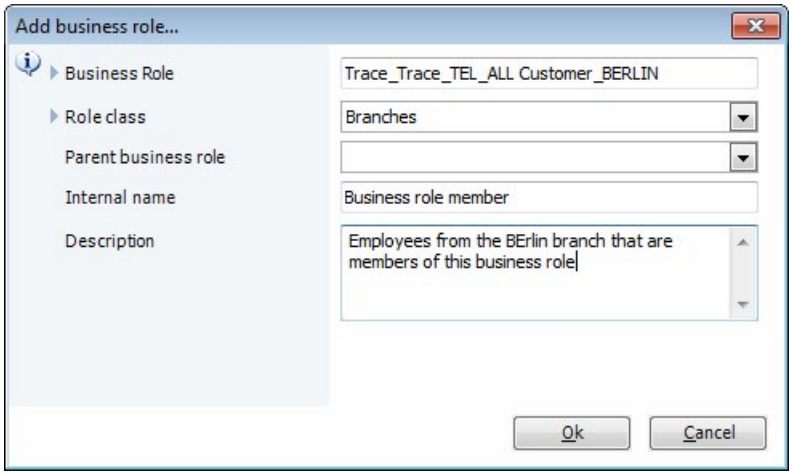
Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

Bookmark Employee for Tracking

To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

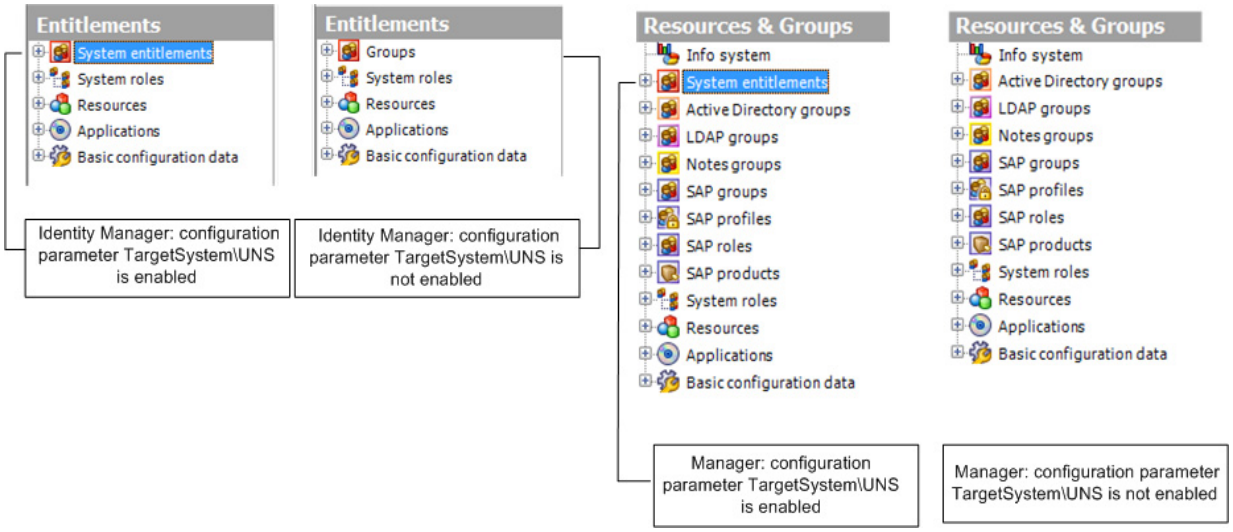
- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

System Entitlements, Groups, Applications

The categories <Resources & Groups> in Manager and <Entitlements> in Identity Manager also show system entitlements, target system groups and application if the appropriate configuration parameters are enabled.

Figure Showing IT Resources in Identity Manager and Manager in the category <Entitlements> or <Resources & Groups>



At this point in Manager, you can edit master data for system entitlements, target system groups and application and also apply task to the objects. You can find detailed information about system entitlements insection System Entitlements in the Unified Namespace on page 154. Read the following section for information on individual target systems Lotus Notes Groups on page 330, Groups, Profiles and Roles Administration on page 383, LDAP Groups on page 418. The section Setting Up Applications on page 124 in the Service Management Manual tells you how to set up applications.

At this point in Identity Manager, you can prepare system entitlements, target system groups and application s for IT Shop requests. To do this, login with a role based authentication module from the application roles <IT Shop>\<Administrators>. You can edit the input field <Service items> and the options <IT Shop> and <Only use in IT Shop> and run the tasks <Add to IT Shop> and <Remove from all shelves (IT Shop)>. There is more information about this in the section Preparing Products for Requesting on page 33 in the IT Shop Manual.

6

Managing Applications

- Introduction
- Editing Applications
- Deleting Applications
- Setting Up and Sharing Application Packages
- Installation Order and Physical Software Dependencies

Introduction

Identity Manager offers convenient administration of applications and their distribution to users and workststations on the network. In this way in, applications can be assigned, for example, to an employee at department level. If an employee logs on to a workstation, the application in installed.

Editing Applications

Standard Configuration Parameters for Software Administration

CONFIGURATION PARAMETER	ACTIVE MEANING
Application	Preprocessor parameter to control the model parts for application administration. If the parameter is active, application administration items are available. If the parameter is changed the database needs to be recompiled.

You can setup applications in the Manager. Applications can be grouped into application packages. Applications and application packages are assigned to employees. The assignments can be made directly or indirectly by assigning to roles. Applications and application packages can be requested from the IT Shop.

You can edit applications in the category <Software> in the Manager.

Basic Data for Setting Up Applications

You can enter basic data for applications <Software> in the filter <Basic configuration data>. The following basic data is required for setting up an application:

- Language
  Certain languages are already available as standard in Identity Manager. You can, however, enter a new langauage.

- Application types
  You can setup further classifications for applications.

Setting Up Applications

Configuration Parameters for Application Administration

CONFIGURATION PARAMETER	ACTIVE MEANING
Software\Application\Group\Prefix	Prefix for identitfiying the application sections.
Software\Application\ShowWithoutProfile	Activating this parameter effects the display of applications that can be assigned and sites.

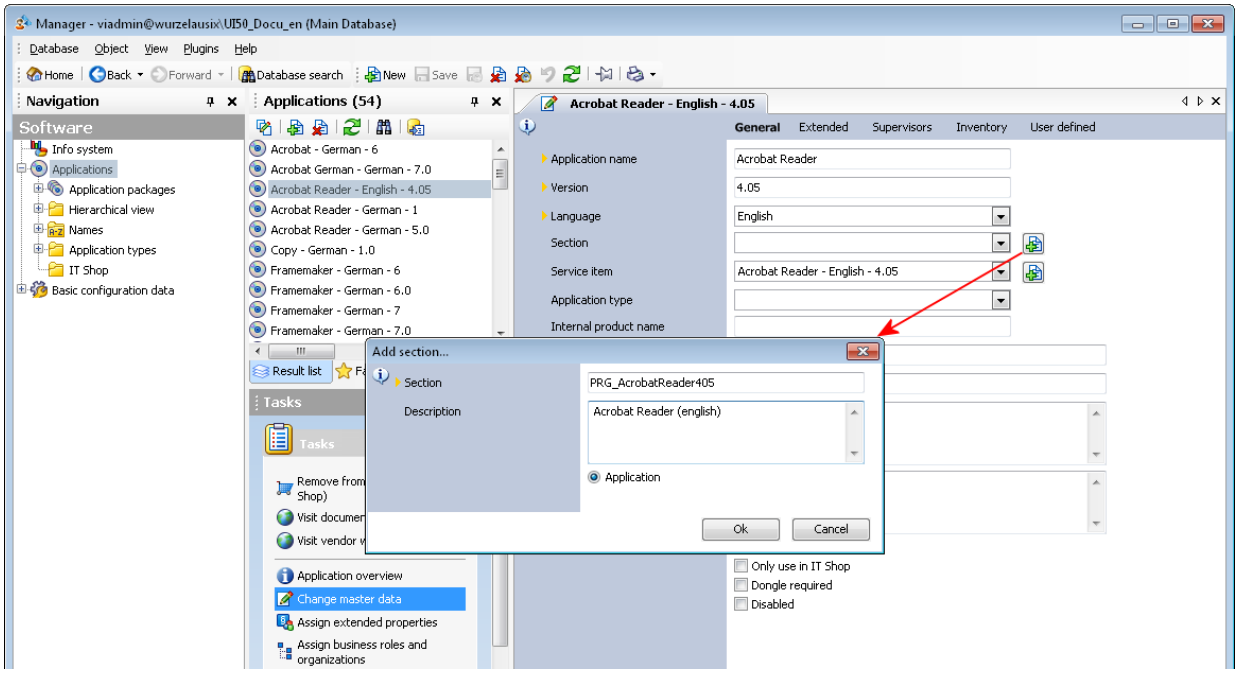
Enter a application in the category <Software>\<Applications>. Applications are filter by different criteria in this category. Ensure that you fill out all the mandatory fields when you edit the master data.

General Master Data for an Application

Enter the application name, version and language on the <General> tab. To extend the classification you can assign an application type to the application. Further optional input concerns the internal product names, website with product information, software documentation as well as the application description. Use the appropriate task from the task view to show the suppliers website or documentation.

In order to distribute the software, a unique application group needs to be set up for each application. This is done using the application specific section that you create with the insert button next to the <Section> option on the application master data form. A dialog window opens where you can enter the section name and a short description. Please ensure that the option <Application> is set.

Setting Up a New Section for an Application



Applications that can only be ordered via the IT Shop are marked with the option <IT Shop>. These applications can be ordered by an employee over the web front-end and distributed using a defined authorized method. However the application can still be directly assigned to employees and non-IT Shop roles. In oder to prevent a direct assignment, set the option <Only use in IT Shop>. In this case the application can only be ordered via the IT Shop. In addition, in order to use an application within the IT Shop, you need to assign an service item to the application or, if necessary, add a new one with the insert button nex to the input field. This means that the ordered applications can be booked internally.

Using the option <deactivated>, you can specify if the application is in use or not. Only applications that are active can be assigned within the Identity Manager database. If an application is deactivated the assignment of the application is not permitted but existing assignments remain intact.

Extended Master Data for an Application

You can add further information relevant to the application installation, for example, the type of installation, change cycle, access types or the current state of use. The permitted values are pre-defined by us, however, you can alter them in the Object Browser to be company specific. In addition, you can enter the operating systems that are supported.

Persons in Charge

On the <Supervisors> tab enter the employees that are responsible for the application. That includes, for example, the department head, the IT manager and their deputies, the coordinator.

Application Inventory Data

Enter the necessary information for stocktaking, for example, usage period and internal stock price for the application. This information can be included in the performance calculation if necessary. If a company's own software is being dealt with, you can set the option <Company software>.

User Defined Master Data

Any further company specific information can be entered on the <User defined> tab. You can tailor the display names, formats and formatting rules for the input fields (default <Spare field no. 01> to <Spare field no.10> to meet your requirements.

Additional Tasks for Managing Applications

After you have entered the master data, you can apply different tasks to the application. You can see the most important information about a application on the overview form. The task view contains different forms with which you can run the following tasks.

Assign System Roles

Applications can be added to various system roles. A system role that only includes applications can be labeled with the system role type "applicaiton package". For more infomations refer to section Setting Up and Sharing Application Packages on page 127 for more information.

Assign Applications to Employees and Company Structures

Application are inherited by employees through assignments to business roles, departments, cost centers and locations. Indirect assignment is the default method for distributing applications. Use the form <Assign to business roles and organizations> to make assignments to individual company s. You can assign applications directly to employees using the appropriate form in order to react quick to special requirements.

When assigning applications, the configuration parameter "Software\Application\ShowWithoutProfile" has to be taken into account. If the parameter is set, assignments can be made even though a profile is not available for the application. If the configuration parameter is not set, the application can only be assigned if a productive profile is available on the FDS.

The current inheritance mechanism and the computation of the application assignments as carried out by the DBScheduler, are described in detail in the Configuration Manual, in section How Employees Inherit Applications on page 280.

Add Applications to the IT Shop

When an application is assigned to an IT Shop shelf it can be ordered by the shop's customers. To ensure the applicaiton is orderable there are further prerequisites need to be guaranteed. There is more information about this in the section Requestable Products on page 33 in the IT Shop Manual. To remove a appliation from the IT Shop, use the task <Remove from all shelves (IT Shop)>.

Assign Extended Properties to an Application

Extended properties are meta objects for which there is no direct mapping, such as accounting codes, controlling areas or cost center areas, in the Identity Manager data model. These extended properties

are used to check rule conformity. For more information see section Setting Up Extended Properties on page 424.

Specify Installation Dependencies for an Application

Use the form <Specify installation dependencies> to enter the order of installation and the physival dependencies of application. Read section Installation Order and Physical Software Dependencies on page 127 for more information.

Deleting Applications

An application can only be deleted when it is no longer assigned to an employee or a business role. An application can be deleted using the context menu in the result list or the button in the toolbar. After the deletion has been confirmed, the application is deleted from the database. The application profile, the section and the application groups are also deleted.

Setting Up and Sharing Application Packages

You can create individual application packages for employees and roles in the Manager. This greatly simplifies application distribution. Application packages are system roles with the system role type ”Application packages“. Employees can obtain application packages directly or by inheriting them over company structures. It is also possible to request application packages through the IT Shop. Applications where the option <Only for use in IT Shop> is enabled can only be assigned to application packages that also have this option set.

You can set up application packages in Manager in the category <Software>\<Applications>\<Application packages>. You can also set up application packages in Identity Manager in the category <Entitlements>\<Applications>\<Application packages>. To do this, log in with a role based authentication model in the application role <IT Shop>\<Administrators>. The system role type <Application package> is preset. Applications can also be added to system roles that are not application packages. For more information about how to set up and share application packages, read the section Editing System roles on page 115.

Established inheritance mechanisms and DBScheduler calculation of application package assignments is described in detail in the Configuration Manual in section How Employees Inherit Applications on page 280.

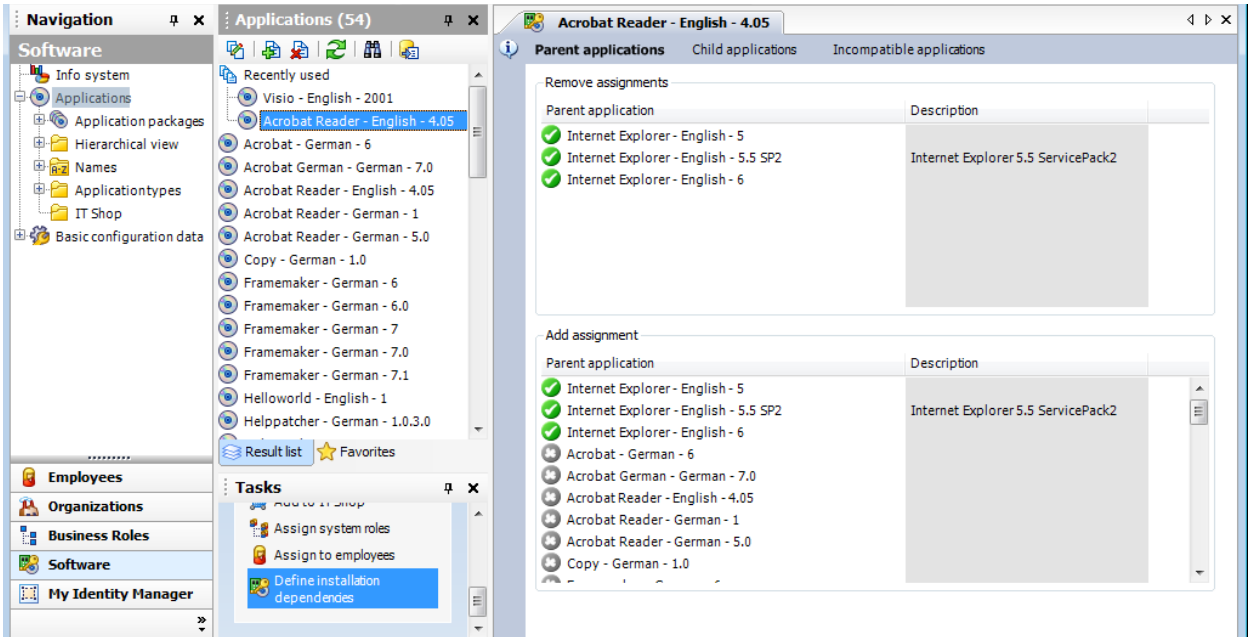
Installation Order and Physical Software Dependencies

With help from the Identity Manager, you can specify the physical dependencies of applications. Dependencies are divided into logical and physical. You can define logical dependencies when you want to specify which applications should be additionally installed in association with a application installation. You can specify incompatibilities in the same way to avoid two incompatible applications being installed for a user. Specify the physical dependencies when a particular installation sequence has to followed or when an application requires another application as installation prerequisite. This might be the case for patches or service packs, for example.

Editing Logical Dependencies

You can specify the dependencies between applications on the form <Define installation dependencies>. Specify a parent application (higher-level) or child (lower-level) for the selected application.

Specify the Installation Dependencies for an Application



Editing Physical Dependencies

Physical dependencies affect the order of installation of applications on the one hand and the installation prerequisites described below on the other.

Editing Software Installation Prerequisites

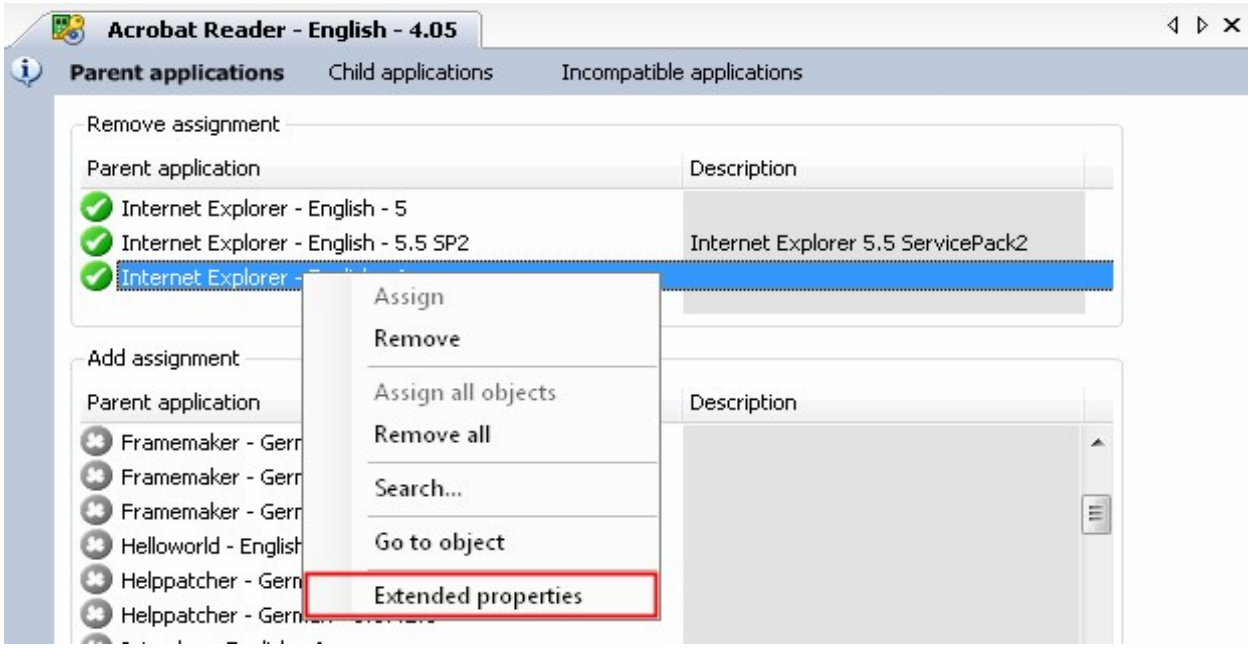
Effective Configuration Parameters for computing Physical Dependencies

CONFIGURATION PARAMETER	MEANING
Software\Application\InheritePhysicalDependencies	This parameter determines the computation of the physical dependencies between software. If the parameter is set, the physical dependencies between applications are taken into account when the DBScheduler computes the number of inherited items (tables *HasAppTotal and *HasDrvTotal). If the parameter is not set, the pysical dependencies are not taken into account in the computation.

In addition to the logical dependency definitions you can specify which software products need to be installed with an application.

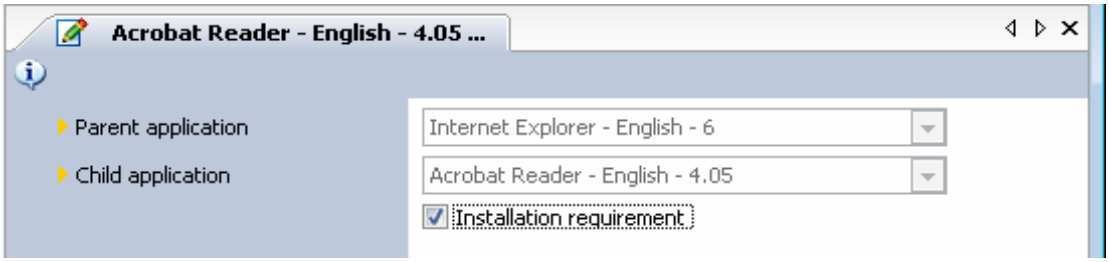
First, specify the (parent) application on the form <Define installation dependencies>. This means that the dependency is set and the sort order can be calculated. After saving the assignment you can change to the detail form via the context menu item <Extended attributes>.

Swap to Detailed Assignment Form



Set the option <Installation prerequisites> for dependency. This means that the required application must be installed before the selected application.

Defining Installation Prerequisites for an Application


Acrobat Reader - English - 4.05 ...
Parent application
Internet Explorer - English - 6
Child application
Acrobat Reader - English - 4.05
Installation requirement

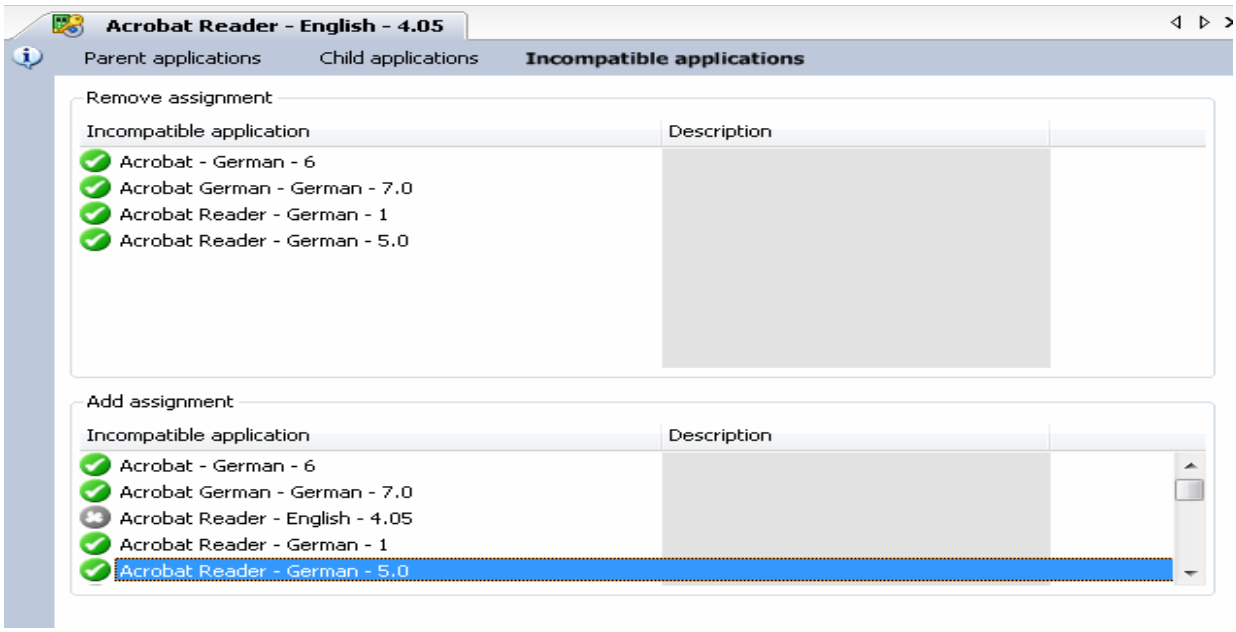
If the parameter ”Software\Application\InheritePhysicalDependencies“ is set, the physically dependent software products are indirectly inherited when an application is assigned to an employee. The computation of the inheritance is done by the DBScheduler.

Editing Self-Excluding Software

You can create an exclusion list for applications that should not be installed together on a workstation because of problems that my occur in functionality.

Specify the (conflicting) applications that you want to exclude for a particular application using the form <Define installation dependencies>.

Specifying Applications to Exclude



The dependencies are evaluated by the DBScheduler.

7

The Unified Namespace

- Introduction
- Unified Namespace Basics
- Unified Namespace Configuration
- Container Structures in the Unified Namespace
- User Accounts in the Unified Namespace
- System Entitlements in the Unified Namespace

Introduction

Unified Namespace is a virtual target system that can map different target systems and their container structures, user accounts, target system groups and corresponding memberships. Through the Unified Namespace, a general, cross target system representation is attained of the connected target system data. Target systems such as Active Directory, Lotus Notes, SAP R/3 and LDAP can represented as well as the customer's own applications such as a telephone system.

By implementing the Unified Namespace other core functions in the Identity Manager can be used across the target systems such as compliance checking, attestation or IT Shop. The Unified Namespace allows other technologies to be used for data synchronization apart fromthe Identity Manager's own target system synchronization.

Unified Namespace Basics

The Identity Manager offers two different ways to manage target systems.

- Full Managment
  In this case, objects for the target systems Active Directory, Lotus Notes, SAP R/3and LDAP are mapped to Unified Namespace as well as the Identity Manager data model and can can be automatically synchronized with the target systems. You can limit full management of individual target system areas, for example, to just an AD domain.

- UNS Management
  In this case, objects for the target systems Active Directory, Lotus Notes, SAP R/3 and LDAP are only mapped to Unified Namespace. Automatic synchronization by the Identity Manager is not intended.

The target system objects are mapped via containers, user accounts and system entitlements in Unified Namespace.Each Unified Namespace object type unifies different the Identity Manager data model tables that are required for mapping the connected target systems.
In addition, each object type references a base table for the target systems that cannot be directly mapped via the Identity Manager data model. If the target systems Active Directory, Lotus Notes, SAP R/3 or LDAP only managed through UNS, the data for these target systems is also mapped via base tables.

Diagram of Target Systems by Unified Namespace Object types

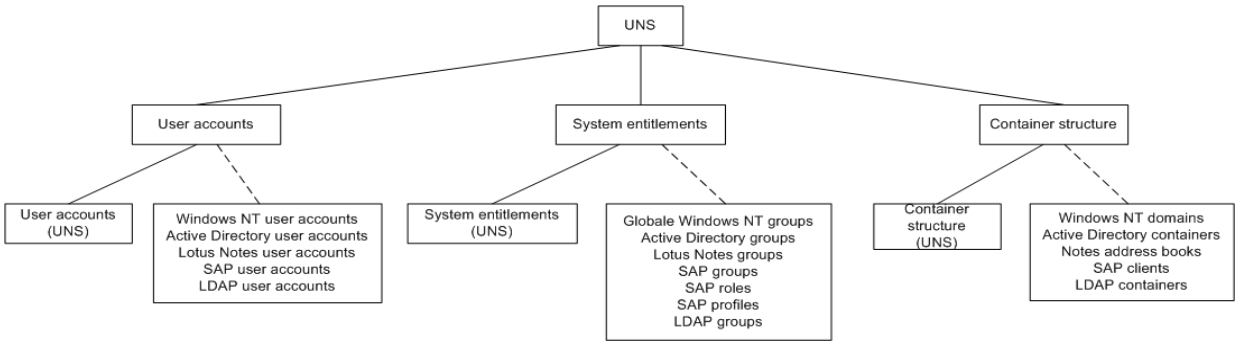
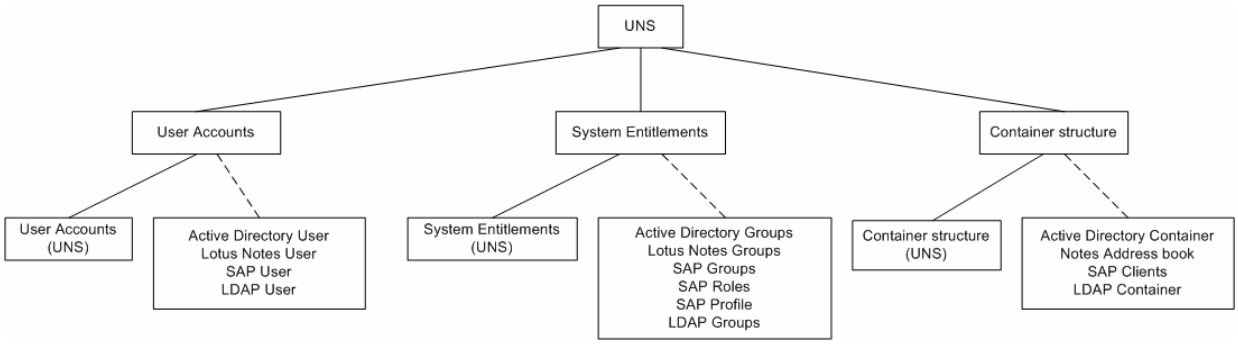


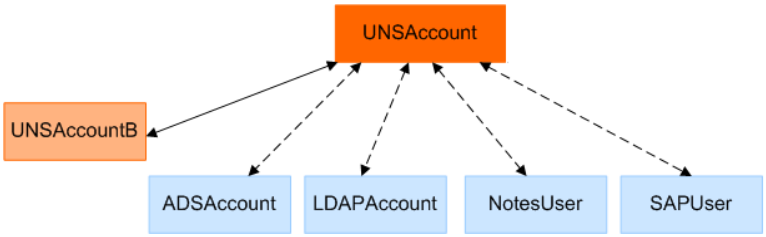
Diagram of Target Systems by Unified Namespace Object types



Each Unified Namespace object has a target system type that specifies exactly which target system the object is assigned to. There are fixed types defined for the target systems Active Directory, Lotus Notes, SAP R/3, LDAP and Windows NT.

The following example shows the Unified Namespace functionality based on mapped user accounts.

Mapping User Accounts in the Unified Namespace

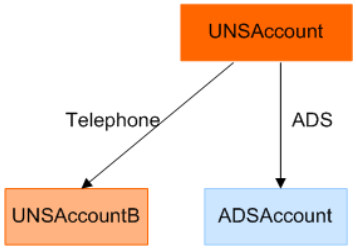


The target system types ”ADS“ for the target system Active Directory and ”Telephone“ for the target system ’telephone’ are defined in the Unified Namespace. User accounts are created in the Unified Namespace by data import. The telephone system data is always diverted to the base table for the user accounts (table ”UNSAccountB“).

The followings options apply for mapping Active Directory user accounts:

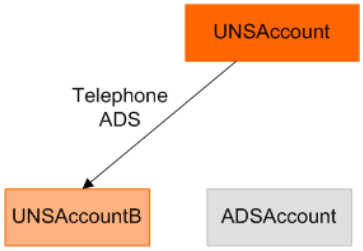
1. Active Directory target system is fully managed in the Identity Manager. The configuration parameter ”TargetSystem\ADS“ is set. The tables for mapping this target system are therefore available in the Identity Manager data model and the imported Active Directory data is mapped to the corresponding target system table (”ADSAccount“). The data for the target system ”Telephone“ is diverted to the base table ”UNSAccountB“.

User Account Mapping in the Unified Namespace (Case 1)



2. The administration of the target system Active Directory carried out via UNS. That means the configuration parameter ”TargetSystem\ADS“ is not set. The tables for mapping the Active Directory target system are therefore not available in the Identity Manager data model and the imported Active Directory data is diverted to the base table ”UNSAccountB“.

User Account Mapping in the Unified Namespace (Case 2)



Advice for Enabling a Target System in the Identity Manager

Take note of the following points if you use Unified Namespace for mapping user accounts and system entitlements of one the target systems Active Directory, Lotus Notes, SAP R/3 or LDAP and want to manage the target system fully with the Identity Manager at a later date:

- In order to manage a target system in the Identity Manager, enable the associated configuration parameters and compile the Identity Manager database. This activates all the tables in the Identity Manager data model and the processes required for mapping the target system. Additional categories for managing the data are displayed in the Manager user interface.
- The existing data from the Unified Namespace base tables is not automatically transfered to the target system in the Identity Manager data model.
- To avoid inconsistant data states between target system tables and Unified Namespace base tables, you need to ensure that the data with the corresponding target system type is transfered from the base tables to the target system tables.
- If only individual target system areas of a target system should be managed with the Identity Manager, for example, only single domains in an Active Directory environment, then the data from the disabled target system areas in the Unified Namespace are labeled with a new target system type. Even this step always has to be custom implemented.

You can find all the other information about data transfer to and from the target system in the section Data Synchronization in Identity Manager on page 161 and the relevant chapter for each individual target system in this manual.

Advice for Full Management of Target Systems in the Identity Manager

Selected properties of the target system objects are mapped in the Unified Namespace user account, system entitlement and container master data. In order to fully map target system objects in the Identity Manager, use full management of the target systems Active Directory, Lotus Notes, SAP R/3 or LDAP. Take the following into account. This also applies when you only manage individual target systems fully in the Identity Manager.

You can modify user accounts, system entitlements and containers not only

- in the category <Unified Namespace>

but also

- in the category for each individual target system.

In the process, only select properties of the target system objects are displayed in Unified Namespace. Therefore, target system objects can only be edited to a limited extent in the Unified Namespace. For example, you can assign a target system type but not a domain to a user account resource. This could cause corrupt or inconsistent data in the target system tables.

Always edit target system objects in the target system categories Active Directory, Lotus Notes, SAP R/3 or LDAP!

Use the Unified Namespace to map objects properties for all target systems on a homogenous basis and to apply other basic Identity Manager functions to the target system objects.

The following sections tell you about the object properties which are mapped in the Unified Namespace.

Unified Namespace Configuration

Configuration Parameters for using the Unified Namespace

CONFIGURATION PARAMETER	MEANING
TargetSystem\UNS	Preprocessor relevant configuration parameter for controlling the model components for managing the unified namespace. If the parameter is set, the target system components are available. Changes to the parameter require compiling the database.

Prerequisite for using the Unified Namespace is that the configuration parameter ”TargetSystem\UNS“ is enabled. This configuration parameter is a preprocessor relevant configuration parameter. This means that the database has to be recompiled after changes have been made to the parameter. For more information see sections Compiling an Identity Manager Database on page 100 in the Getting Started Manual and Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual.

Unified Namespace target system types, containers, user accounts and system entitlements are displayed in the category <Unified Namespace>.

Setting Up Target System Types in the Unified Namespace

Target system types are used to distinguish different target system data in the Unified Namespace. Each object that is mapped in the Unified Namespace has a target system type. This ID is used to decide which table is required to map the data.

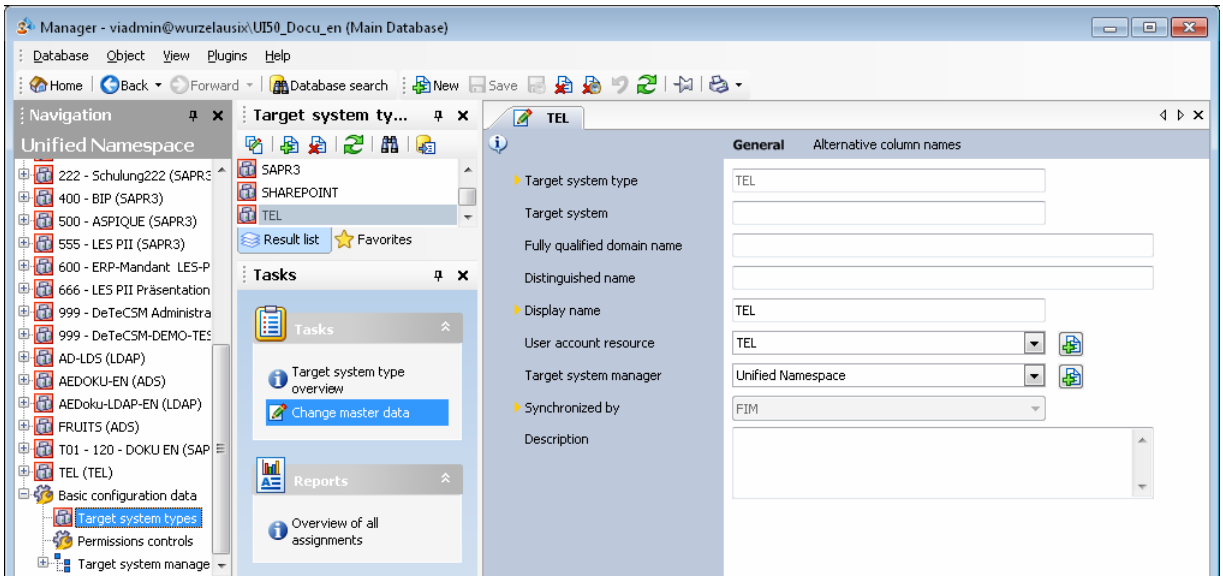
There are fixed target system type defined for mapping the target systems Active Directory, Lotus Notes, SAP R/3, LDAP and Windows NT. You can define more target system types for other target systems as well.

Fixed Target system types

TARGET SYSTEM	TARGET SYSTEM TYPE
Active Directory	ADS
LDAP	LDAP
Lotus Notes	NOTES
SAP R/3	SAPR3

Edit target system types with the Identity Manager in the category <Unified Namspace>\<Basic configuration data>\<Target system types>. To do this, you need to login with a role based authentication module from the application role <Target systems>/<Unified Namespace>

Displaying Target System Types in the Unified Namespace



The following data is required for a target system type:

- Target system type name
- Target sytem
  If there are several target system types allowed for one target system, they are grouped according to the value entered here.
- Display name
  Name that is displayed in the Identity Manager tools for the target system type.
- User account resource
  This input is required when the user account with this target system type is managed via a user account resource in the Unified Namespace. For more information read section Managing Unified Namespace User Accounts with User Account Resources on page 148.
- Target system manager
  Select the Identity Manager application role whose members are responsible for the target system administration with Unified Namespace. You can use the button next to the input field

to create a new application role. Target system managers can only modify those object properties that are displayed in the <Unified Namespace> category. The target system managers only edit the properties that are shown in the category <Unified Namespace>.

- Synchronized by
  Specify the direction for the data to be synchronized between target system and the Identity Manager. Choose between ”FIM“ and ”No synchronization“.

  FIM: data synchronization between the Identity Manager database and the target system is performed by Microsoft Forefront Identity Manager.
  No synchronization: no changes are automatically transfered from the Identity Manager database to the target system.

  You can only specify the type of synchronization when you first add a target system type. After saving, you cannot make further changes. If you specify ”no synchronization“ you can define custom processes to swap data between the Identity Manager and the target system. Specify the type of synchronization for target systems AD, LDAP, Lotus Notes, NT 4 and SAP R/3 based on the target system area for the target system For more detailed information refer to the chapters Managing an Active Directory Environment on page 201, Managing a Lotus Notes Environment on page 295, Managing an SAP R/3 Environment on page 343, Managing Generic Target Systems on page 399.

- Detailed description of the target system type

If you manage target systems „fully“ in the Identity Manager, the target system managers for target system types in Unified Namespace can also edit the same object properties as target system managers for individual target systems, to a limited extent. This can lead to corrupt or inconsistent data in the target system tables.
Always edit target system objects in the target system categories Active Directory, Lotus Notes, SAP R/3or LDAP!

Reports about Target System Types

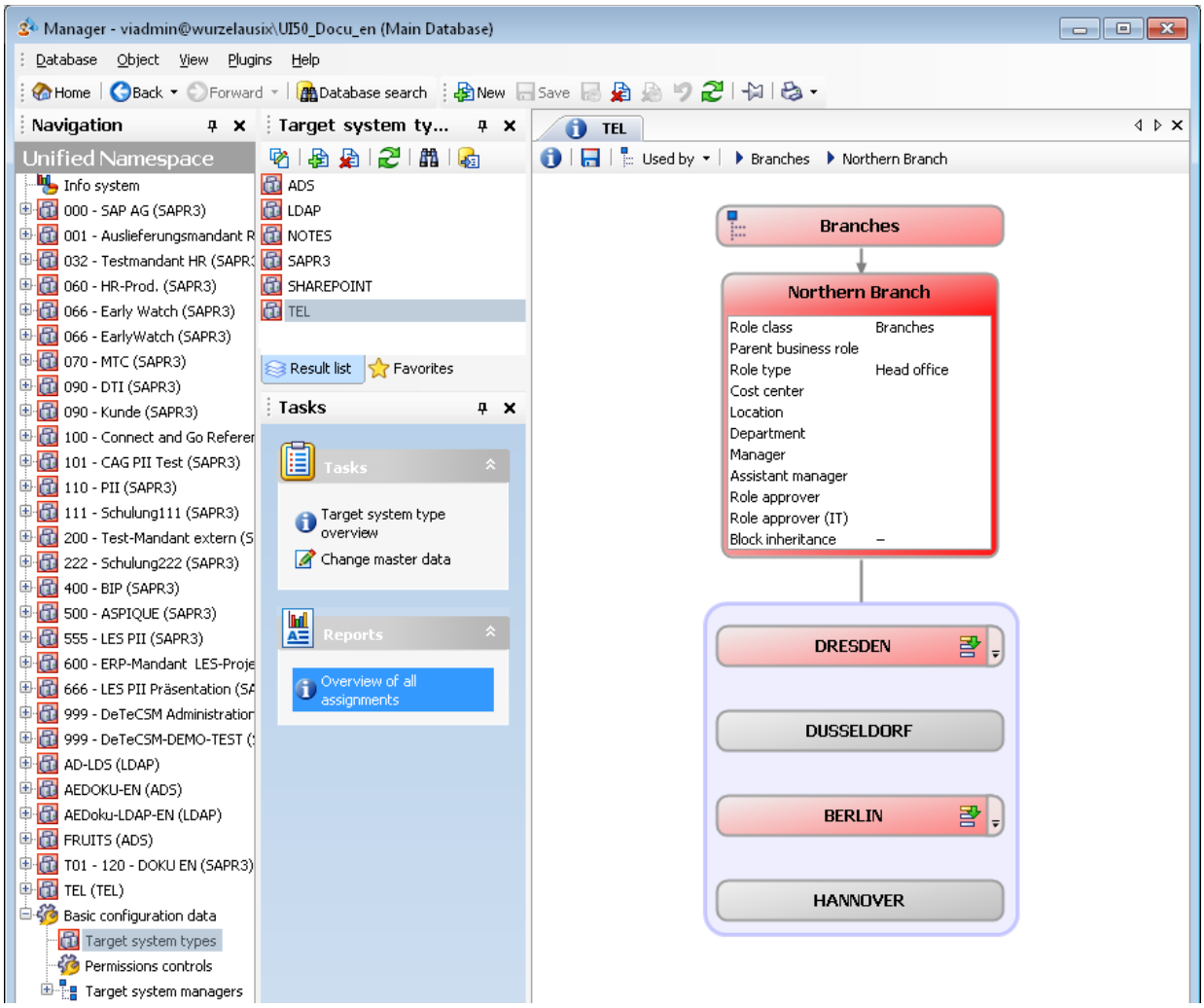
The Identity Manager makes various report available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for target system types.

Overview of All Assignments

This report shows all employees that are assigned to at least one user account in the selected target system type. Directly assigned objects as well as those object inherited by the employee are take into

account in this case. The report shows which roles of a role classe the employee belongs to. What you get is an organigram of the different role classes for the selected target system type.

Report "Overview of all Assignments" for an Target System Type



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees in the selected target system type that have a user account and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

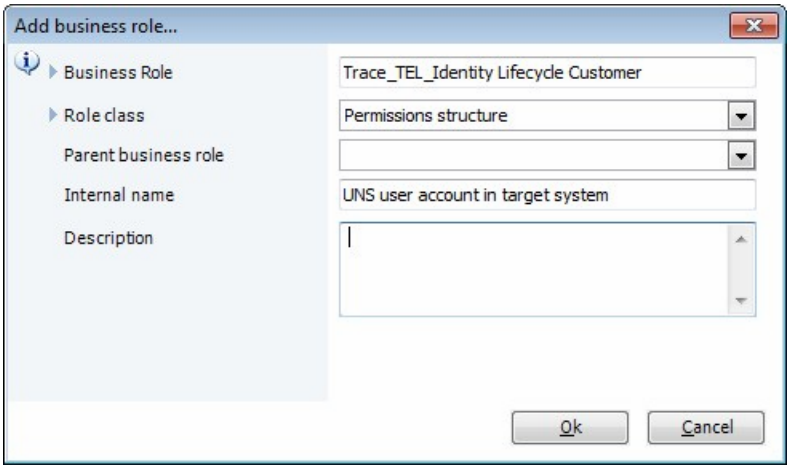
Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

Bookmark Employee for Tracking

To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected target system type and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Target System Manager

In the Identity Manager, you can assign employees that can edit objects for this target system to every target system type. To do this, assign a <target system manager> application role to a target system tyoe in the master data. Assign the employees that are authorized to edit this target system in the Identity Manager to this application role.

Edit target system managers for the unified namespace in the Manager in the category <Unified Namespace>\<Basic configuration data>\<Target system managers>\<Unified Namespace> or in the Identity Manager in the category <Identity Manager Administration>\<Target systems>\<Unified Namespace>. You can find more detailed information about application roles in section The Identity Manager Roles Model on page 61. Read about how to assign target system managers to target system types in section Setting Up Target System Types in the Unified Namespace on page 135.

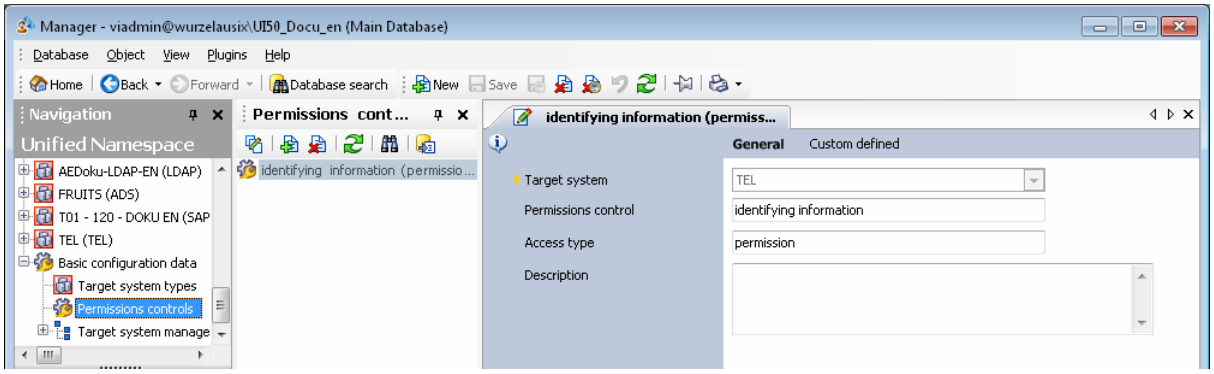
Unified Namespace Permissions Controls

Use permissions controls to map more properties of your own target systems, for example, a telephone system. To do this, you can import the data you want into the Identity Manager from your own target system. Permissions controls can also be added in Identity Manager or Manager.

Edit permissions controls in Identity Manager in the category <Unified Namespace>\<Basic configuration data>\<Permissions controls>. To do this, login with a role baed authentication module from the application roles <Target systems>\<Unified namespace>. You can also edit permissions controls in the Manager.

Permissions Control General Master Data

Permissions Controls General Master Data



The following data is required for a permissions control:

- Permissions control's name
- Access type
- Description
  Text field for your own details about permissions controls

Permissions Controls User Defined Master Data

This tab is used to enter additional customized data for permissions controls. You can use Designer to edit the the display names, formats and templates for the input fields (by default <Spare field no. 01> to <Spare field nr. 10>) to meet your own requirements.

Additional Tasks for Permissions Controls

After you have entered all the setup data, you can apply different tasks to the permissions controls. You obtain the most important information about the permissions control from the overview form. There are various tasks available in the task view that you can use to run the following tasks.

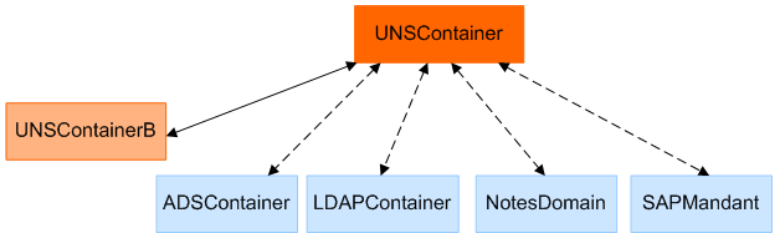
Assign User Accounts and System Entitlements

You can use the tasks <Assign user accounts> and <Assign system entitlements> to assign a permissions control direct to Unified Namespace user accounts or system entitlements.

Container Structures in the Unified Namespace

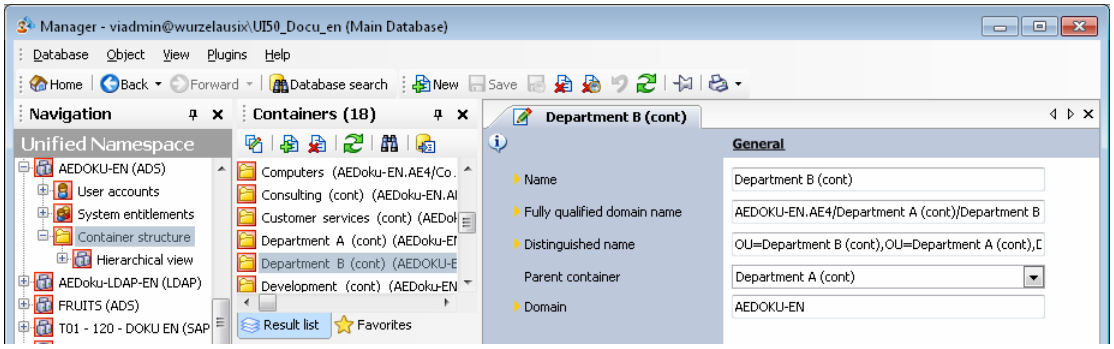
The Unified Namespace container structure represents the structural elements in each of the target systems.

Mapping Containers in the Unified Namespace



The Unified Namespace containers are displayed in the category <Unified Namespace>\<Target systems>\<Container structure>. To do this, login with a role based authentication module from the application role <Target systems>\<Unified Namespace>. You can also edit container structures in the Manager.

Displaying Containers in the Unified Namespace Interface



Enter the following master data for a container in the Unified Namespace:

- Container name
- Fully qualified domain name and defined name of the container
  The fully qualified domain name and defined name of the container are made up from the container name, the target system type and the parent container.
- Parent container
  Enter a parent container to create a hierarchical container structure.
- Domain
  Target system area that the container belongs to.

The following table contains a mapping of Unified Namespace container properties to the corresponding structure elements in each target system.

Unified Namespace Container Properties Mapping

TARGET SYSTEM TYPE	*	ACTIVE DIRECTORY	LDAP	NOTES	SAPR3
UNS-CONTAINER	**UNS-CONTAINERB**	**ADS-CONTAINER**	**LDAP-CONTAINER**	**NOTES-DOMAIN**	**SAPMAN-DANT**
Canonical-Name	CanonicalName	Canonical-Name	Canonical-Name	Canonical-Name	Canonical-Name
CN	CN	CN	CN	FullName	Mandanten-nummer
Distinguished-Name	Distinguished-Name	Distinguished-Name	Distinguished-Name		Distinguished-Name
Ident_Domain	Ident_Domain	Ident_Domain	Ident_Domain	NotesDB	DisplayName
ObjectGUID	ObjectGUID	ObjectGUID	ObjectGUID		
UID_Parent-UNSContainer	UID_Parent-UNSContainerB	UID_Parent-ADSContainer	UID_Parent-LDAPContainer		
UID_UNS-Container	UID_UNS-ContainerB	UID_ADS-Container	UID_LDAP-Container	UID_Notes-Domain	UID_SAP-Mandant

Reports about Container Structures

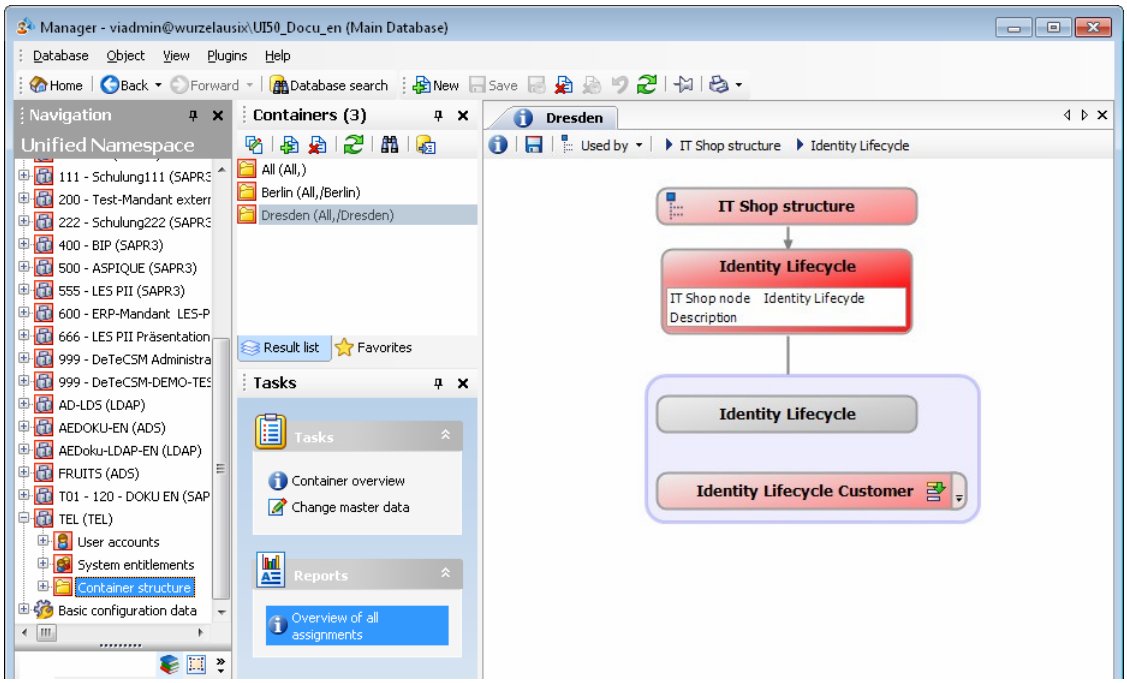
The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for container structures:

Overview of All Assignments

This report shows all employees that are assigned to at least one user account in the selected container. Directly assigned objects as well as those object inherited by the employee are take into account in this

case. The report shows which roles of a role classe the employee belongs to. What you get is an organigram of the different role classes for the selected container.

Report "Overview of all Assignments" for an Container



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees in the selected container that have a user account and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

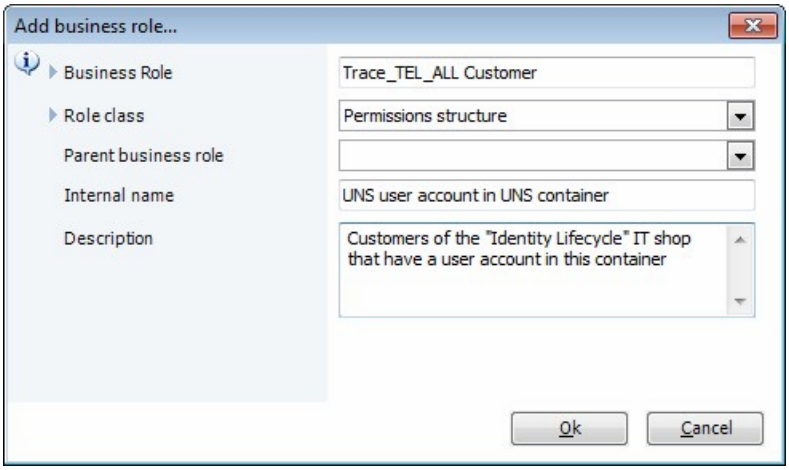
Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

Bookmark Employee for Tracking

To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected container and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

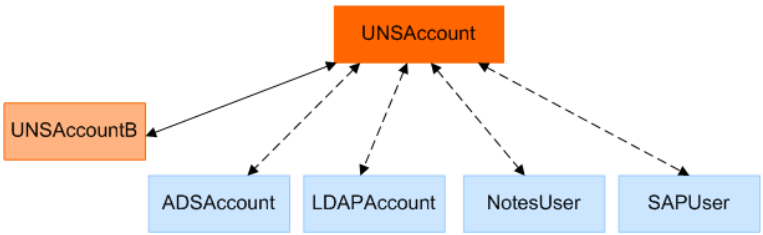
- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

User Accounts in the Unified Namespace

The user accounts in the Unified Namespace represent the user accounts in each of the target system.

Mapping User Accounts in the Unified Namespace



A user account can be linked to an employee in the Identity Manager. Even so you can manage the user accounts separately from employees, for example to map administration user accounts. The Identity Manager works with several methods to create user accounts and to assign user accounts to employees.

- Employees and user accounts can be entered manually and assigned to each other.
- Employees get their user accounts automatically through user account resources. If an employee does not have a user account in a target system, a new user account is created by assigning the user account resource to an employee through the integrated inheritance mechanism and subsequently processing it. This method is described in more detail in the section Managing Unified Namespace User Accounts with User Account Resources on page 148.

The basic mechanisms are dealt with in the chapter Employees and User Accounts on page 25.

In order to set up user accounts for company employees we recommend using user account resources. If a user account resource is used to set up a user account, some of the employee master data described in the following is inherited b the employee’s user accounts via templates. The extent of this is dependent on the default mange level of the user account resource. You can customize the templates supplied.

When you manage user account resources via user accounts, you can specify the way user accounts behave when employees are enabled or deleted. Refer to the section Handling Disabling and Deletion of Employees and User Accounts on page 44 for more information.

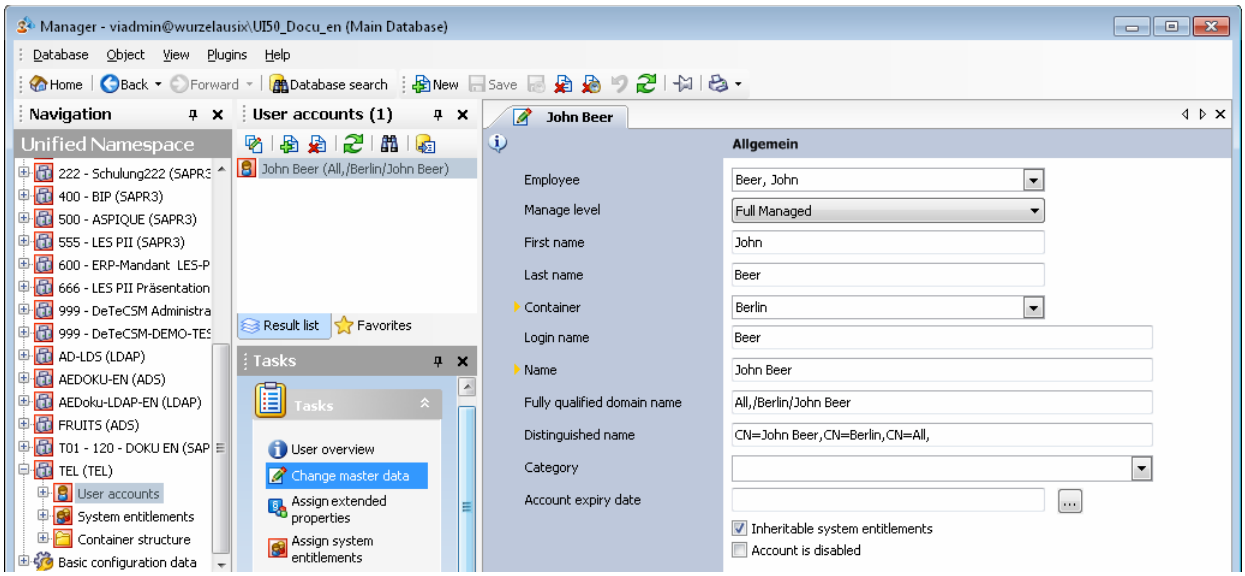
If SAP system users are maintained via a central user administration, these central system users are displayed in Unified Namespace. The associated Unified Namespace user accounts are displayed in the navigation view under both the central system and the client system.

Entering Master Data for Unified Namespace User Accounts

Edit Unified Namespaceuser accounts in Identity Manager in the category <Unified Namespace>\<<Target systems>>\<User account>.To do this, log in with a role based authentication from the application role <Target systems>\<Unified Namespace>. You can also edit user accounts in the

Identity Manager. You can manually enter the required input on the form <Edit master data> and make changes as necessary. Note that all fields marked as compulsory have to filled in.

Displaying User Accounts in the Unified Namespace



Enter the following data for each user accounts in the Unified Namespace:

- Target System
  Select a target system from the drop-down menu. You can only edit this input field when you add an new user account.

- Employee
  Assign a user account to an employee. If the user account was created via a user account resource, the employee is already entered. If you create the user account manually, you can select the employee from the menu.

- User account resource
  Select a user account resource from the drop-down menu. If you have entered an employee in the <Employee> field, the Identity Manager determines the IT operating data for this employee and enters it in the respective input fields for this user account.
  Use the user account to automatically fill the user account input fields and to specify the manage level. To ensure future maintenance of the user account through user account resources, allocate the target system type and the employee to the user account resource.

- Manage level
  Select a manage level from the drop-down menu. You can only enter the manage level when you have already entered a user account resource. The values in the list are dependent on the manage level defined for the selected user account resource. You can find further informationin the section Manage Level for Handling Unified Namespace User Accounts on page 152

- First name, last name, container and login name
  Enter the first and last names and select the container for creating the user account in. If you have assigned a user account resource, the input fields are automatically filled out depending on the manage level.

- Name, fully qualified domain name, defined name
  These are determined via templates.

- Category
  Categories are relevant when unified namespace users should inherit system entitlements. System entitlements can be selectively inherited by the user. To do this, system entitlements and users are divided into categories. User the <Category> drop-down menu to assign one or more categories to a user. The principle of inheritance is explained in detail in the section Inheriting Group Memberships Based on Categories on page 82.

- Account expiry date
  Specify the date up to which the user can log into a target system with this user account. The Identity Manager disallows a login if the date has already passed. If you specify a leaving date for an employee it is used as account expiry date if the appropriate manage level is set. Any existing account expiry date is overwritten in thus case. If you delete an employees leaving date at a later point in time, the user account expiry date remain intact!

- Inheritable system entitlements
  Set this option if you want user accounts to inherit system entitlements via roles. Add an employee with user account to a business role, for example, and if you have assigned system entitlements to this business role then the user account inherits these system entitlements indirectly. Prerequisite for this is that the option <System entitlements> is set for the user account. Inheritance of group membership is described in section How User Accounts Inherit System Entitlements in the Unified Namespace on page 308.

- Account is disabled
  If a user account is not required for a certain period of time, you can temporarily deactivate it with the option <Account is disabled>. If the user account is connected to an employee, the account can also be disabled by disabling or deleting the employee. Read the section Handling Disabling and Deletion of Employees and User Accounts on page 44 for more information on this.

The following table contains the mapping of an Unified Namespace user account properties to user accounts in each target system.

Mapping Unified Namespace User Account Properties

TARGET SYSTEM TYPE	*	ACTIVE DIRECTORY	LDAP	NOTES	SAPR3
UNSACCOUNT	**UNSACCOUNTB**	**ADSACCOUNT**	**LDAPACCOUNT**	**NOTESUSER**	**SAPUSER**
AccountDisabled	AccountDisabled	AccountDisabled	AccountDisabled	AccountDisabled	
AccountExpires	AccountExpires	AccountExpires		IDExpires	Gltgb
CanonicalName	CanonicalName	CanonicalName	CanonicalName	CanonicalName	CanonicalName
CN	CN	CN	CN	CN	Accnt
DistinguishedName	DistinguishedName	DistinguishedName	DistinguishedName	FullName1st	DistinguishedName
FirstName	FirstName	GivenName	GivenName	Firstname	Firstname
IsGroupAccount	IsGroupAccount	IsGroupAccount	IsGroupAccount		
LastName	LastName	Surname	SN	Lastname	Lastname

Mapping Unified Namespace User Account Properties

TARGET SYSTEM TYPE	*	ACTIVE DIRECTORY	LDAP	NOTES	SAPR3
UNSAC-COUNT	UNS-ACCOUNTB	ADS-ACCOUNT	LDAPAC-COUNT	NOTES-USER	SAPUSER
ManageLevel	ManageLevel	ManageLevel	ManageLevel	ManageLevel	ManageLevel
ObjectGUID	ObjectGUID	ObjectGUID	ObjectGUID	ObjectGUID	
UID_Person	UID_Person	UID_Person	UID_Person	UID_Person	UID_Person
UID_UNS-Account	UID_UNS-AccountB	UID_ADS-Account	UID_LDAP-Account	UID_Notes-User	UID_SAPUser
UID_UNS-Container	UID_UNS-ContainerB	UID_ADS-Container	UID_LDAP-Container	UID_Notes-Domain	UID_SAP-Mandant

Additional Tasks for Managing Unified Namespace User Accounts

After you have entered the user account master data you can apply different tasks to the user account. You will find the most important information about the user account on the overview form. There are several forms available in the task view that you can run the following tasks with.

Assign System Entitlements directly to a Unified Namespace User Account

Use this task to assign system entitlements directly to user accounts. You can assign system entitlements that

- belong to the same target system area as the selected user account
- belong to target system areas that trust this target system area.

All Unified Namespace system entitlements that are directly or indirectly assigned to the user account are displayed on the form. Use this form to edit direct assignment of system entitlements. To edit an indirect assignment, change the assignment from employee or system entitlement to roles. Refer to section Assigning Company Resources through Roles on page 78 for more information.

Assign Extended Properties to Unified Namespace User Accounts

Extended properties are meta objects that are not directly mapped in the Identity Manager data model, such as accounting codes, controlling areas or cost accounting areas. Extended properties are used for checking conformity to rules. You can find more information in section Setting Up Extended Properties on page 424.

Managing Unified Namespace User Accounts with User Account Resources

You can use user account resources to automatically create user accounts for company employees in the Unified Namespace. You can set up user account resources for each target system type in the Uni-

fied Namespace. The basic methods are explained in section Creating User Accounts with User Account Resources on page 37.

If an employee should obtain a user account via user account resources, the employee must have a central user account and get the IT operating data via assignment to a primary department, primary location or a primary cost center. Read section Handling Employees and User Accounts on page 30 on how to do this.

When a user account resource is assigned to an employee, the default installation checks whether the employee already has a user account with the target system type of the user account resource. If no user account exists, a new user account with the user account resource's default manage level is created. If a user account does exist but it is disabled then it is reenabled. In this case you have to change the user account manage level afterwards.

You can specify exactly one user account resource per target system type. If an employee has more than one user account with the same target system type, add more user accounts using the master data form. For this, you need to define other manage level for the user account resource that the target system type is assigned to. You can select manage levels on the user account master data form. Refer to section Manage Level for Handling Unified Namespace User Accounts on page 152 for more information.

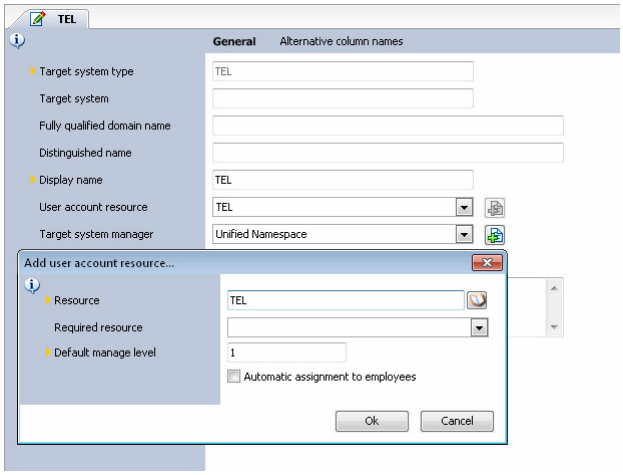
Setting Up a User Account Resource

Configuration Paramater for User Account Resources

CONFIGURATION PARAMETER	MEANING
TargetSystem\UNS\UniqueDefaultManageLevel	When the parameter is set, a different default manage level is expected for each user account resource in Unified Namespace (default). If the parameter is not set, each user account resource in the Unified Namespace may have the same default manage level.

Set up a user account resource for a target system type Identity Manager in the category <Unified namespace>\<Baisc configuration data>\<Target system types>. To do this, login with a role base authentication module from the application role <Target systems>\<Unified namespace>. You can also setup resources in Manager. Enter a new user account resource using the button next to the input field <User account resources> on the target system type master data form.

Setting Up a User Account Resource for a Target System Type

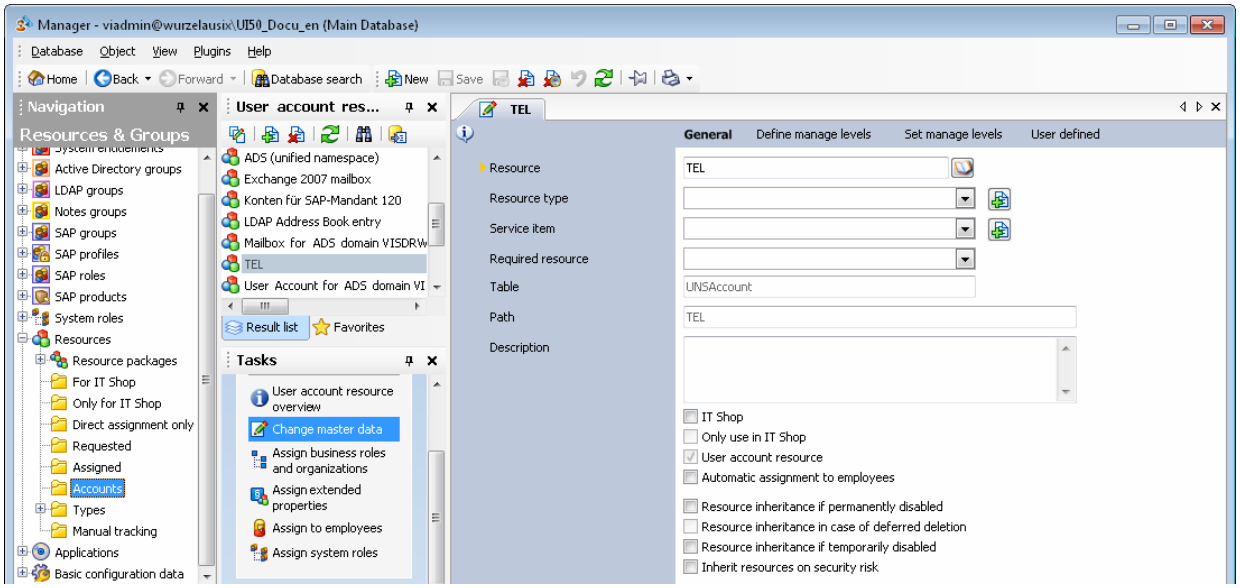


Enter the following data for the user account resource:

- Resource name
- Predefined resource
  Dependencies between user account resources are defined here.
- Default manage level
  Specify the default manage level that should be used when a new user account is added using this user account resource. Enter the value ”1“ in order to create user accounts with the manage level ”Full manged“.
  A different default manage level is expected in the standard Identity Manager installation for every user account resource that is used in Unified Namespace. You have to disable the configuration parameter TargetSystem\UNS\UniqueDefaultManageLevel if you want to create a separate user account resource with the default manage level ”full managed“.
- Automatic assignment to employees
  Label the user account with this option when the user account resource should be automatically assigned to all internal employees. On saving, the user account resource is allocated to each person that is not marked as external. New employees automatically obtain this user account resource as soon as they are added. The DBScheduler calculates the assignment.

Once the input is saved, a new user account resource is created. Edit the other data for this user account resource afterwards in Identity Manager the category <Entitlements>\<Resources> in the filter <Accounts>. You can also edit user resource account in Manager in the category <Resources & Groups>\<Resources> in filter <Accounts>.

Post-processing User Account Resources



Addition user account data is:

- Resource type
  Resources should contain a resource type. This resource type determines subsequent processing steps of a resource request or assignment. You can also setup resources in Manager. Enter a new resource type using the button next to the input field.
  If you are working with the Identity Manager, add new resource types in the category <Entitlements>\<Basic configuration data>\<resource types> with a user from the application role <IT Shop>/<Administrators>.

- Service item
  Assign an existing service item to the user account resource or add a new one. This allows the user account resource to be requested fromthe IT Shop.
  If you are working with the Manager, add new service items in the category <IT Shop>\<Service Catalog>\<Requestable service items> with a user from the application role <IT Shop>/<Administrators>.

- Table
  The base table for mapping the user accounts
  This input is preset with the value ”UNSAccount“ when the user account resource is assigned to a target system type and cannot be edited.

- Path
  The path of the domain that should be used for the user account resource
  This input is preset with the value ”UNSAccount“ when the user account resource is assigned to a target system type and cannot be edited.

- Description
  Spare text field for writing your own information about the user account resource

- IT Shop usage
  Label a user account resource that can be requested through the IT Shop (see Chapter Setting Up an IT Shop Solution on page 15). with the option <IT Shop>. This user account resource can be requested by the company employees via the IT Shop and allocated through a defined approval procedure. The user account resource can, however, still be assigned directly to employees and roles. To prevent this, enable the the option <Only for use in IT Shop>. The only allows the user account resource to be requested through the IT Shop.
  If you set this option, assign a service item to the user account resource. This allows the user account resource to be added to the IT Shop.

- User account resource
  Labels the selected resource as user account resource. This option cannot be changed.

- Automatic employee assignment
  Label the user account resource with this option when it should be automatically assigned to all employees. The user account is assigned to every internal employee on saving. The moment a new employee is added, they also are assigned this user account.The assignment is computed by the DBScheduler.

- Resssource inheritance
  Define the user account resource inheritance behavior for every user account resource itself. The inheritance options of possible predecessor resources are overwriiten in this case. You might want disabled employees to inherit user account resources to ensure that all the necessary system entitlements are quickly available if they are enabled at a later date, for example. You can set the following options.
  Resource inheritance if ...

...permanently disabled:	Option set: if an employee is permanently disabled, the user account resource remains assigned to them. The user account is disabled. Option not set: the user account resource is no longer inherited by the employee. The associated user account is deleted.
...deferred:	Option not set: if the employee is labeled for deletion, the user account resource assignment is removed from the employee. The associated user account is deleted. This option cannot be enabled.

...temporarily disabled:	Option set: if an employee is temporarily disabled, the user account resource remains assigned to the employee. The user account is diabled. Option is not activated: the user account resource is no longer inherited by the employee. The associated user account is deleted.
...security risk:	Option set: if an employee poses a security risk, the user account remains assigned to them. The associated user account is disabled. Option not set: the user account resource assignment is removed from the employee. The associated user account is deleted.

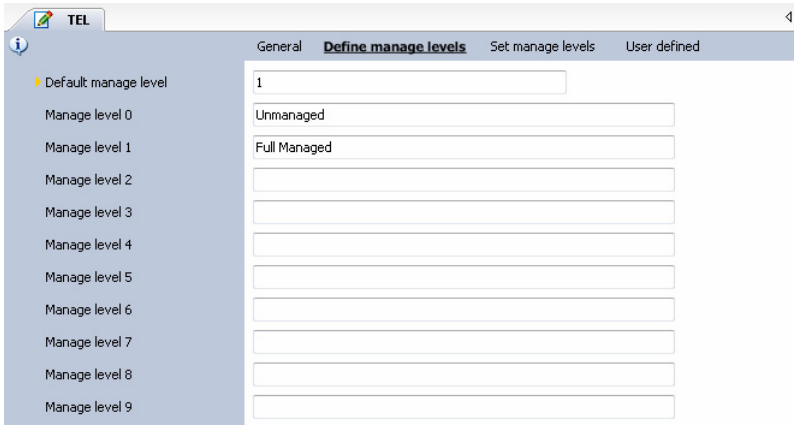
Manage Level for Handling Unified Namespace User Accounts

Specify the manage level for a user account resource for managing the user accounts. The manage level of a user acount is determined by the amount of employee properties inherited by the user account.

The Identity Manager supplies configurations for the manage levels ”Unmanaged“ and the ”Full managed“. User accounts with the manage level ”Unmanaged“ are linked to an employee but do not inherit further properties. User accounts with the manage level ”Full managed“ inherit specific properties from the assigned employee. Manage levels are taken into account in the value templates, which are used to find user account attributes. You can define other manage levels depending on your requirements.You need to ammend the value templates to include manage level approaches.

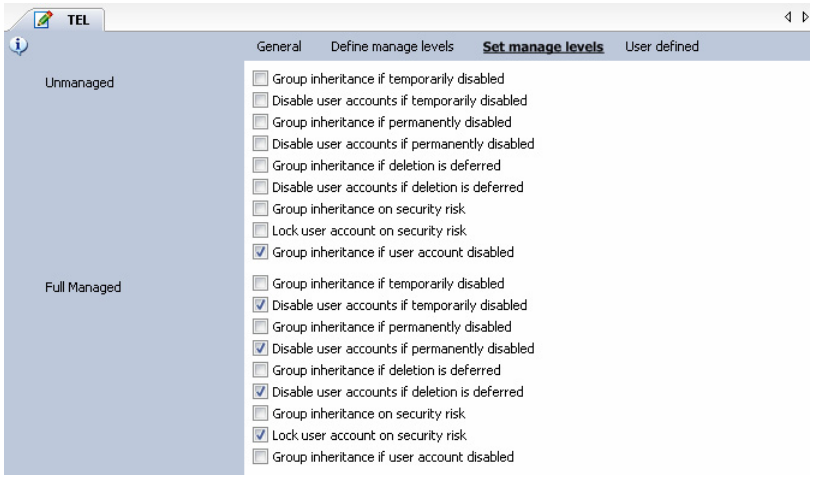
Specify a default manage level for every user account resource. The default manage level is used when a new user account is added via a user account resource. You can assign one user account resource for every target system type. In the default installation, a different default manage level is expected for each user account resource. However, the Identity Manager allows several user account resources to be used with the default manage level. Use the configuration parameter ”TargetSystem\UNS\UniqueDefaultManageLevel“ to control the behavior you want. You can find more information and examples in the section Creating User Accounts with User Account Resources on page 37.

Manage Levels for User Account Resources



Use the <Set manage levels> form to specify the effects that temporary disabling, permanent disabling, deletion and the security risk of an employee have on their user account and group memberships for each manage level.

Edit User Account Resource Manage Levels


TEL
General
Define manage levels
Set manage levels
User defined
Unmanaged
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled
Full Managed
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled

An employee's user accounts can be locked in order to remove their system entitlements when the employee is diabled or deleted. If the employee is reenabled at a later date, the user accounts are also reenabled. This behavior is controlled by the properties:

- Disable user accounts if permanently disabled
- Disable user accounts if temporarily disabled
- Disable user accounts if deletion is deferred
- Disable user accounts on security risk

Group membership inheritance can be specified for the user account resource target system area. You may want to discontinue inheritance when an employee's uer account is locked and can therefore not be a member of a group, for example. During this period inheritance should not be calculated for this employee. Existing group memberships are therefore deleted! This behavior is controlled by the properties:

- Group inheritance if permanently disabled
- Group inheritance if temporarily disabled
- Group inheritance if deletion is deferred
- Group inheritance on security risk

You will find further information in section Handling Disabling and Deletion of Employees and User Accounts on page 44.

Deleting User Account Resources

You can delete user account resource if they are not assigned to a target system type. Proceed as follows:

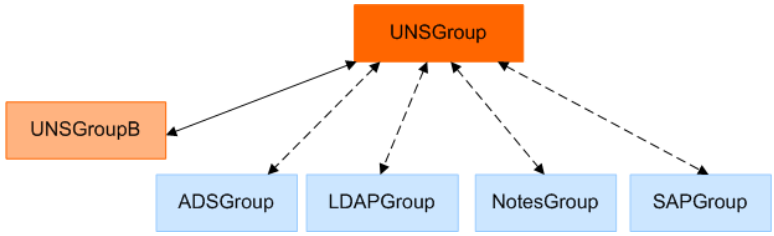
1. Start Identity Manager or Manager

2. Remove user account resource assignments to target system types
3. Start Manager
4. Select category <Resources & Groups>\<Resources>\<Accounts>
5. Select the user account resource in the result list and delete it

System Entitlements in the Unified Namespace

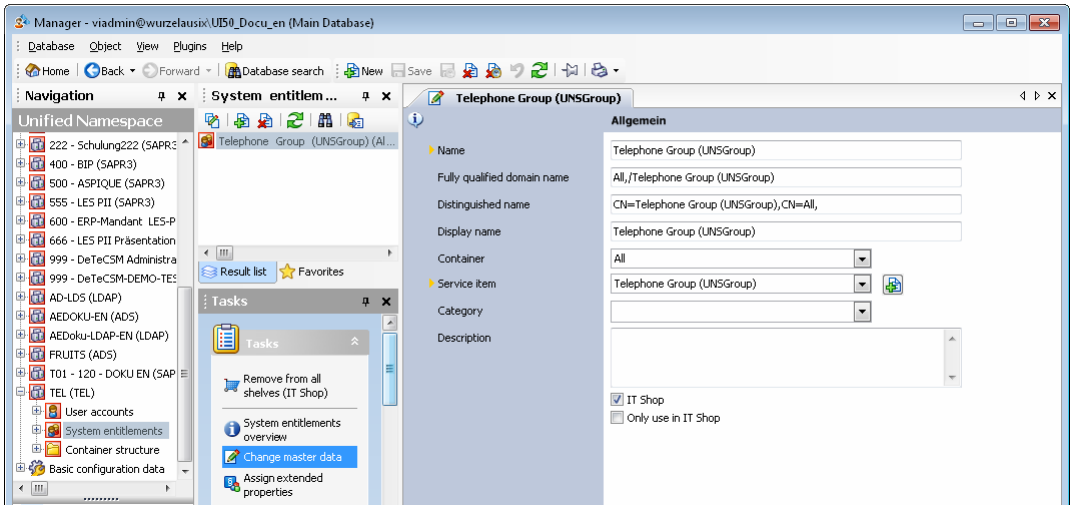
System entitlements in the Unified Namespace represent groups in each of the target systems.

Mapping Groups in the Unified Namespace



Edit system entitlements in Identity Manager in the category <Unified Namespace>\<Target systems>\<System entitlements>. To do this log in with a role based authentication module from the application role <Target systems>\<Unified Namespace>. You can also setup system entitlements in Manager.

Displaying System Entitlements in the Unified Namespace



Enter the following master data in the Unified Namespace for the system entitlement:

- Name of the system entitlement and the display name
- Full qualified domain name and defined name
  The full qualified domain name and the system entitlement defined name are determined using templates from the system entitlement name and the container name.

- Container
  Select the container that the groups to contain the system entitlement.

- Service item
  In order to request system entitlements via IT Shop, assign an existing service item to it or add a new one. You can find more detailed information about service items in the section Preparing Products for Requesting on page 33 in the IT Shop Manual.
  If you are working with Identity Manager, allow addition of new service items in the category <Accounting>\<Service items> via a user with the application role <IT Shop>\Administrators>.

- Permissions category
  UNS user accounts can selectively inherit system entitlements. To do this, system entitlements and user accounts are divided into categories. Use the <Permissions category> list to assign one or more categories to a system entitlement. The principles of inheritance are described in detail in the section Inheriting Group Memberships Based on Categories on page 82.

- Description
  Spare text field for your own description about system entitlements

- IT Shop
  Label a system entitlement that can be requested via the IT Shop with the option <IT Shop>. This system entitlement can be requested by the company employees via the IT Shop and allocated through a defined approval procedure. The system entitlement can, however, still be assigned directly to employees and roles. To prevent this, enable the the option <Only for use in IT Shop>. In this case, the system entitlement can only be requested via the IT Shop.
  If you set this option, assign a service item to the system entitlement. This allows the system entitlement to be added to the IT Shop.

The following table contains the mapping of an Unified Namespace system entitlement properties to groups in each target system.

Mapping Unified Namespace System Entitlement Properties

TARGET SYSTEM TYPE	*	ACTIVE DIRECTORY	LDAP	NOTES	SAPR3
UNSGROUP	**UNSGROUPB**	**ADSGROUP**	**LDAPGROUP**	**NOTES-GROUP**	**SAPGROUP**
CanonicalName	CanonicalName	CanonicalName	CanonicalName	CanonicalName	CanonicalName
CN	CN	CN	CN	DisplayName	GroupName
DistinguishedName	DistinguishedName	DistinguishedName	DistinguishedName	ListName1st	DistinguishedName
IsForITShop	IsForITShop	IsForITShop	IsForITShop	IsForITShop	IsForITShop
IsITShopOnly	IsITShopOnly	IsITShopOnly	IsITShopOnly	IsITShopOnly	IsITShopOnly
ObjectGUID	ObjectGUID	ObjectGUID	ObjectGUID	ObjectGUID	
UID_AccProduct	UID_AccProduct	UID_AccProduct	UID_AccProduct	UID_AccProduct	UID_AccProduct

Mapping Unified Namespace System Entitlement Properties

TARGET SYSTEM TYPE	*	ACTIVE DIRECTORY	LDAP	NOTES	SAPR3
UNSGROUP	UNSGROUPB	ADSGROUP	LDAPGROUP	NOTES-GROUP	SAPGROUP
UID_UNS-Container	UID_UNS-ContainerB	UID_ADS-Container	UID_LDAP-Container	UID_Notes-Domain	UID_SAP-Mandant
UID_UNS-Group	UID_UNS-GroupB	UID_ADS-Group	UID_LDAP-Group	UID_Notes-Group	UID_SAP-Group

Additional Tasks for Managing System Entitlements

After you have entered the master data you can apply different tasks to the system entitlement. You will find the most important information about the system entitlement on the overview form. There are several forms available in the task view that you can run the following tasks with.

Assign Business Roles and Organizations

Tools: Identity Manager, Manager

If a system entitlement is assigned to a role, it becomes possible for a user account to inherit it. System entitlements are added to departments, cost centers, locations or roles. If you add an employee to these roles and they have a user account with the <System Entitlements inheritable> option set, the user account is assigned the system entitlements. You can find further information in the section Assigning Company Resources through Roles on page 78.

The inheritance procedures are calculated by the DBScheduler. System Entitlements inheritance is described in section How User Accounts Inherit System Entitlements in the Unified Namespace on page 308 in the Reference Manual.

Assign System Roles

Tools: Manager

A system entitlement can be added to different system roles. When a system role is assigned to employees, all the unified namespace user accounts that these employees own inherit the system entitlements. System entitlements with the option <Only for use in IT Shop> can only be assigned to system roles that also have this option set. For more information about system roles see section System Roles on page 114.

Established inheritance mechanisms and calculation of system role assignments by the DBScheduler is described in detail in the Configuration Manual in section System Role Inheritance on page 283.

Assign User Accounts

Tools: Identity Manager, Manager

Use this task to assign user accounts directly to system entitlements. You can assign user accounts that

- belong to the same target system area as the selected system entitlement
- belong to target sytem areas that trust this target system area

All Unified Namespace user accounts that are directly or indirectly assigned to the user account are displayed on the form. Use this form to edit direct assignment of user accounts. To edit an indirect assignment, change the assignment from employee or user account to roles. Refer to section Assigning Company Resources through Roles on page 78 for more information.

Assign System Entitlements

User this task to assign Unified Namespace system entitlements directly to a system entitlement. You can assign system entitlements that

- belong to the same target system area as the selected system entitlement
- belong to target sytem areas that trust this target system area

Use the form <Is member of> to assign parent system entitlements of the selected system entitlement. User the form <Has members> to assign child system entitlements of the selected system entitlement.

Specify Inheritance Exclusion

Tools: Identity Manager, Manager

Use the form <Specify inheritance exclusion> to define dependencies between system entitlements. The number of user account memberships in groups is limited by the definition of system entitlement dependencies. You can assign system entitlements that

- belong to the same target system area as the selected system entitlement
- belong to target sytem areas that trust this target system area

Read more about dependencies between system entitlements in section Inheritance Exclusion on page 80.

Add System Entitlements to the IT Shop

Tool: Manager

System entitlements can be requested by a shop customer when they are assigned to an IT Shop shelf. There are more prerequisites required for requesting system entitlements. See section Requestable Products on page 33 for more information. To remove system entitlements from the IT Shop use the task <Remove from all shelves (IT Shop)>.

Assign Extended Properties to System Entitlements

Tools: Identity Manager, Manager

Extended properties are meta objects that are not directly mapped in the Identity Manager data model, such as accounting codes, controlling areas or cost accounting areas. Extended properties are used for checking conformity to rules. You can find more information in section Setting Up Extended Properties on page 424.

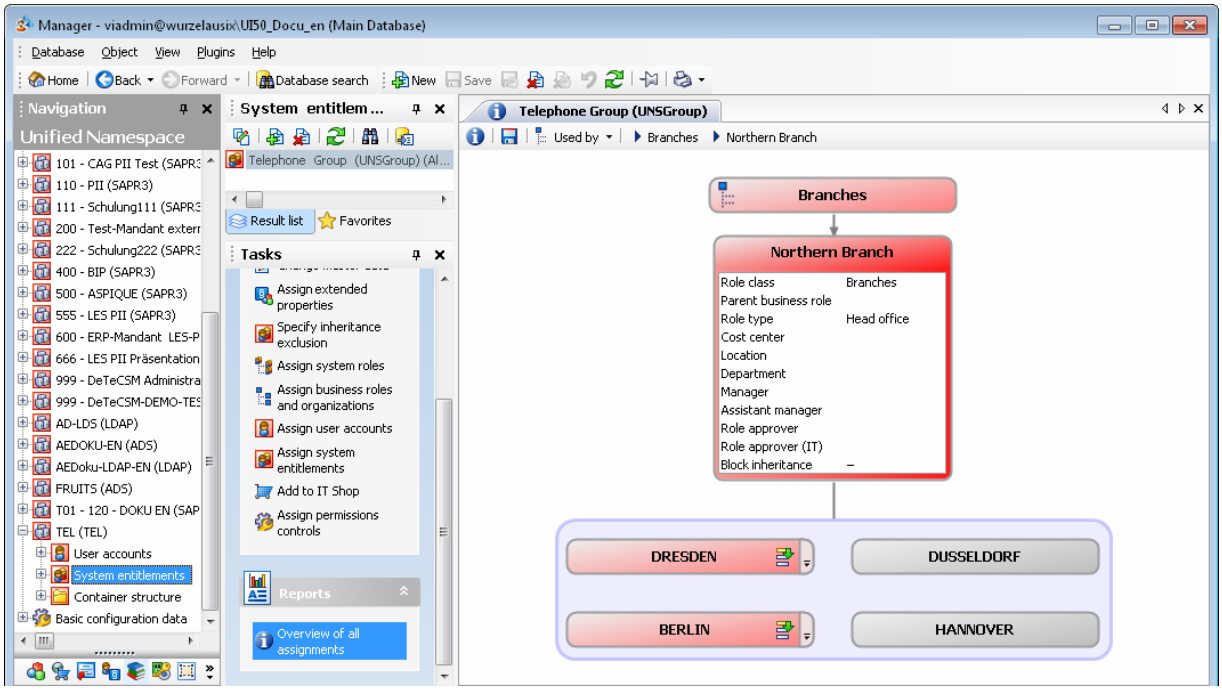
Reports about System Entitlements

The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for the selected system entitlements:

Overview of All Assignments

This report shows all employees that are assigned one user account with the selected system entitlement. Directly assigned objects as well as those object inherited by the employee are take into account in this case. The report shows which roles of a role classe the employee belongs to. What you get is an organigram of the different role classes for the selected system entitlement.

Report "Overview of all Assignments" for an Container



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees in the selected system entitlement that have a user account and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

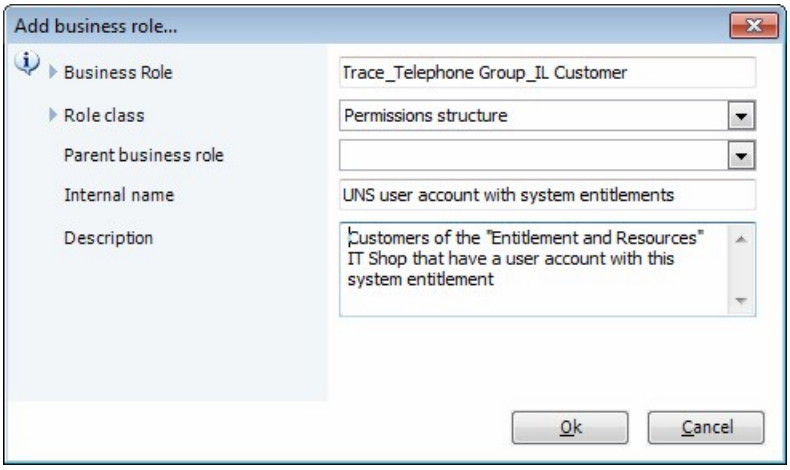
Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

Bookmark Employee for Tracking

To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

8

Data Synchronization in Identity Manager

- Introduction
- Synchronisation by Identity Manager
- Customizing Mapping rules
- Synchronization Server Administration

Introduction

When target systems are connected to Identity Manager for the first time, the target system objects and their properties must be transfered to the Identity Manager database. The same thing applies if objects or their properties are modified in the target system environment. The data can be synchronized by various methods.

Synchronization by:

- Identity Manager
  Identity Manager Service is responsible for synchronizing data between the Identity Manager databank and the target system environment. See section Synchronisation by Identity Manager on page 162 for more information.

- Microsoft Forefront Identity Manager (FIM)
  Microsoft Forefront Identity Manager is responsible for synchronizing data between the Identity Manager database and the target system environment.

- Customizedprocess
  Customized processes are define for synchronizing data. See section Defining Processes on page 46 in the Process Orchestration Manual on how to define custom processes in Identity Manager.

The method for data synchronization is determined when a target system is added in Identity Manager. Refer to the following sections for more information General Master Data for an Active Directory Domain on page 206, General Master Data for a Lotus Notes Domain on page 307, General Master Data for a Client on page 352, General Master Data for an LDAP Domain on page 404. The type of synchronization for the target system cannot be changed afterwards.

Synchronisation by Identity Manager

Target system administration primarily takes place over the Identity Manager database. Actions relevant to the target systems such as insertion, modifcation or deletion of a user account in the database are transferred automatically and in realtime. Different processes are defined on the target system objects for this. These are executed the moment an insert, delete or update event occurs. On the grounds of security, target system relevant objects are never deleted from the Identity Manager database automatically or before issuing a request.

If object properties are directly changed in the target system environment on top of that, then data inconsistencies occur between the target system and the Identity Manager database. These inconsistencies can be corrected by running data synchronization with Identity Manager on a regular basis. To do this, you need to define several synchronization configurations. Scheduled tasks are used to synchronize objects specified in the synchronization configuration between Identity Manager and the target system are fixed times. Identity Manager also uses other synchronization methods to correct data inconsistencies between Identity Manager and the target system. Synchronization is carried out via scheduled tasks.

Configure synchronization with the Manager for each target system domain of each target system. You need to have the following prerequisites to be able to configure synchronization for a target system domain:

- The field <Synchronized by> on the master data form for the target system domain must contain ”Identity Manager“.

- The system user logged into Manager must be allocated the permissions group ”VID“.
  Alternative: If you apply custom permissions groups, assign the system user a permissions group with edit permissions for the tables ”DialogSchedule“ and ”JobAutoStart“.

- The schema and mapping rules for the target system to be synchronized have been loaded into Identity Manager.

A synchronization server must be installed and declared in the Identity Manager database so that the Identity Manager can execute a synchronization. For more information read section Synchronization Server Administration on page 196.

Loading Target System Schema and Mapping Rules

Tool: Manager

Before you can configure synchronization, you have to load the target system schema and the mapping rule for mapping target system properties in data model in the Identity Manager database. To do this run the tasks <Load schema> and <Load mapping rule> for the target system domain. You are notified when each process has started.

There is a target system mapping rule embedded in the process components. These are loaded on initial synchronization and stored in the database column ”MappingInfo“ for the synchronized target system domain. If there is a mapping rule given on the <Synchronization> tab, which is on the master data form for that target system domain, it is merged with the internal process component mapping rule. The mapping rule that results is stored in the database. Synchronization can be configured once this process has been handled by Identity Manager Service.

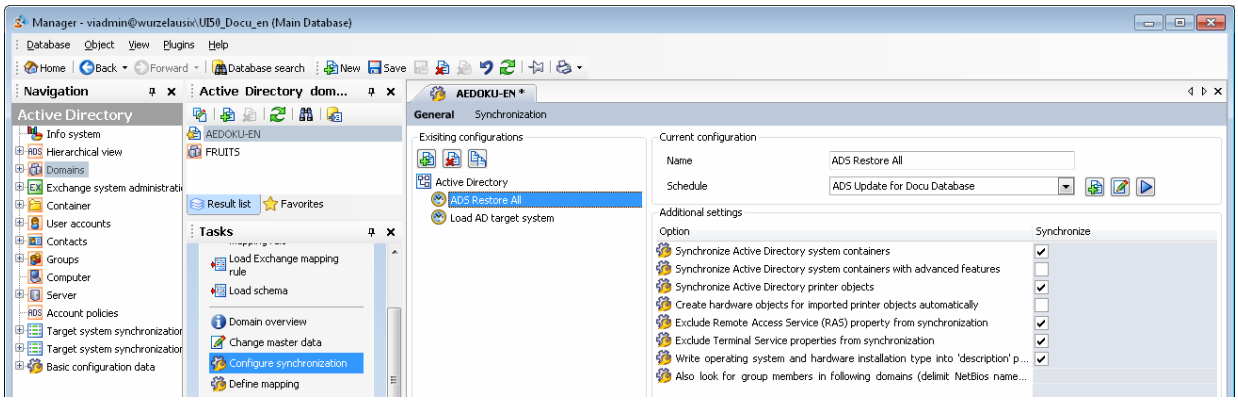
You are notified if there are already mapping rules or schema in the database. You can overwrite mapping rule stored in the database or the existing schema.

How to Configure Synchronization

Tool: Manager

Use the task <Configure synchronization> to create a synchronization configuration.

Synchronization Configuration Master Data



Different synchronization configurations are displayed on the <General> tab.

Existing Configurations

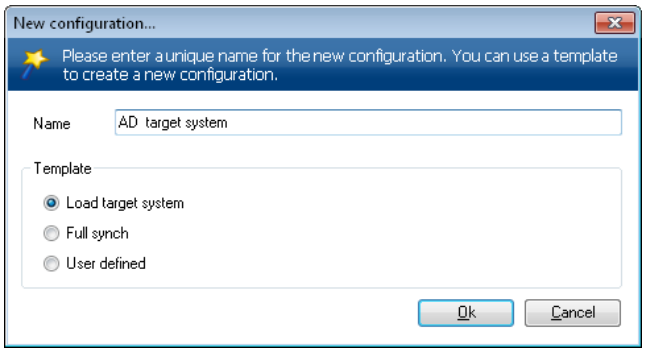
All synchronization configurations are listed in the <Existing configurations> pane and can be selected for editing from there

Meaning of Icons in the <Existing configurations> Pane

ICON	MEANING
	Create new synchronization configuration.
	Delete selected synchronization configuration.
	Copy selected synchronization configuration.
	A schedule is assigned to the synchronization configuration. The schedule is enabled.
	A schedule is assigned to the synchronization configuration. The schedule is not enabled.

If you want to create a new synchronization configuration you get help from Identity Manager in selecting object types and assignments to synchronize and the behavior of the synchronization. Certain object types/assignments and their synchronization behavior are preselected via templates. Then you can edit these settings.

Create Synchronization Configuration



Enter a name for the synchronization confiuration and select a template.

- Load target system
  All target system objects and assignments are selected for synchronization. Objects that only exist in the target system are added to Identity Manager. Objects that only exist in Identity Manager are not synchronized. Object properties that exist in both target system and Identity Manager are not synchronized.

- Full sync
  All target system objects and assignments are selected for synchronization. Objects that only exist in the target system are added to Identity Manager. Objects that only exist in Identity Manager are marked for deletion. Object properties that exist in both target system and Identity Manager are updated.

- User defined
  There are no object types and assignments selected for synchronization. Object types/assignments and synchronization behavior must be entirely custom defined.

The templates for full sync vary depending on the target system. Synchronization behavior can vary from the basic behavior described above for individual objects. check the object types/assignment and the synchronization behavior anyway before you save the synchronization configuration.

Current Configuration

You can edit the selected synchronization configuration in the <Current configuration> pane. You can

- Change the name of the selected synchronization configuration
- Assign a schedule

Use the drop-down menu to select one of the existing system schedules. Use the buttons next to the <Schedule> input field to set up a new schedule, edit the assigned schedule and start synchronization schedule.

Meaning of Icons in the <Current configuration> Pane

ICON	MEANING
	Create a new schedule.
	Edit assigned schedule.
	Start the synchronization schedule for the selected synchronization configuration.

Create and edit schedules for the synchronization configuration using the buttons mentioned. Synchronization can only be started if the assigned schedule is enabled.

- When a schedule is executed, all the synchronization configurations are executed that the schedule is assigned to!
- If one schedule is assigned to more than one synchronization configuration a unique process is generated for each synchronization configuration. This can delay processing of an individual process.
- Before you assign mulitple schedules check the effects on process handling.
- Before you start a schedule manually, check whether other processes are executed that are processed where appropriate by the Identity Manager Service beforehand.

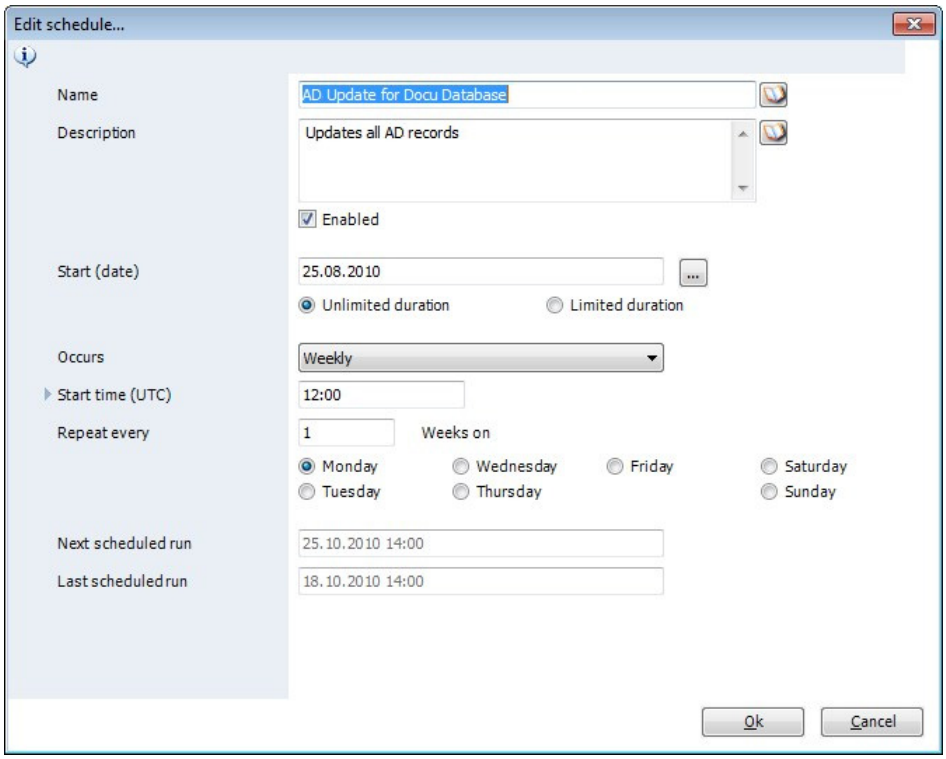
The advice given above is also valid if a schedule is manually started using the <Start schedule> button! If one schedule is assigned to more than one synchronization configuration a unique process is generated for each synchronization configuration. If these processes are handled one after the other by

the Identity Manager Service (for example SAP components), handling of individual processes can be delayed because the order is selected randomly. The maximum number of instances for the respective process components determines whether processes are handled simutaneously or in sequence. For more information see section Process Components on page 79 in the Process Orchestration Manual.

Creating and Editing Schedules

Use schedules to start scheduled tasks. There is a scheduled task stored for every synchronization configuration that is assigned a schedule. You can find detailed information about this in chapter Setting Up Scheduled Tasks on page 73 in the Process Orchestration Manual.

Schedule for Starting Synchronization



The following common properties are required for a schedule:

- Name
  Unique name for the schedule.

- Description
  Detailed description of the schedule

- Enabled
  If this option is set, the scheduled task is started at the next possible point in time. The target system domain is snychronized.
  If the option is not set the scheduled task is not run. The target system domain is therefore not synchronized.

Use the following setting to configure execution times for the schedule:

- Validity period
  Use the options <Unlimited duration> and <Limited duration> and the <Start (date)> and <End (date)> fields to specify a valid interval for the scheduled task. Enter the first day on which the scheduled task should be run and the last day it should be run.

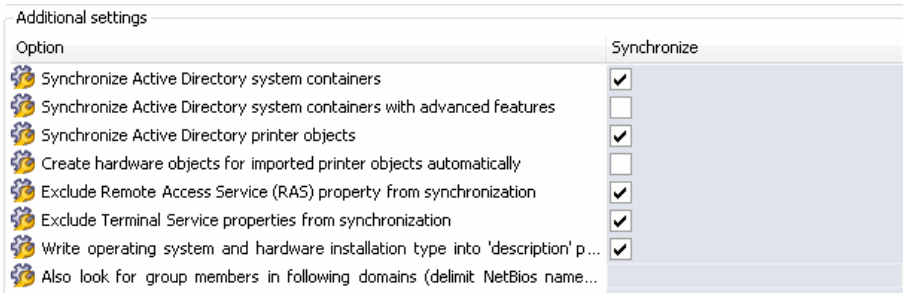
- Run interval for task
  Specify the time interval for running the scheduled task. The starting point is calculated from the frequency (<Repeat every>) and the tyoe of interval (<Occurs>). Minute, hour, day, week, month and year are valid types of interval. For interval types week, month and year you need to specify exactly which day of the week, day of the month or day of the year. Enter the time in UTC.

- Start information
  The start information includes the time for the last scheduled run (<Last scheduled run>) and the time for the next scheduled run (<Next scheduled run>) of the scheduled task. The time of the next run is calculated from the specified start interval. Identity Manager supplies the information in the local time of the client it was started in.

Additional Settings

The <Additional settings> pane allows you to make more modifications to the synchronization. The <Option> column shows a list of different, target system specific synchronization tasks. Use the check box in the <Synchronization> column to select which of these options should be taken into account. Certain options require additional values. Enter these in the <Synchronization> column. If the fields are empty, these synchronization options are not taken into account.

Selecting Option in the Additional Settings Pane

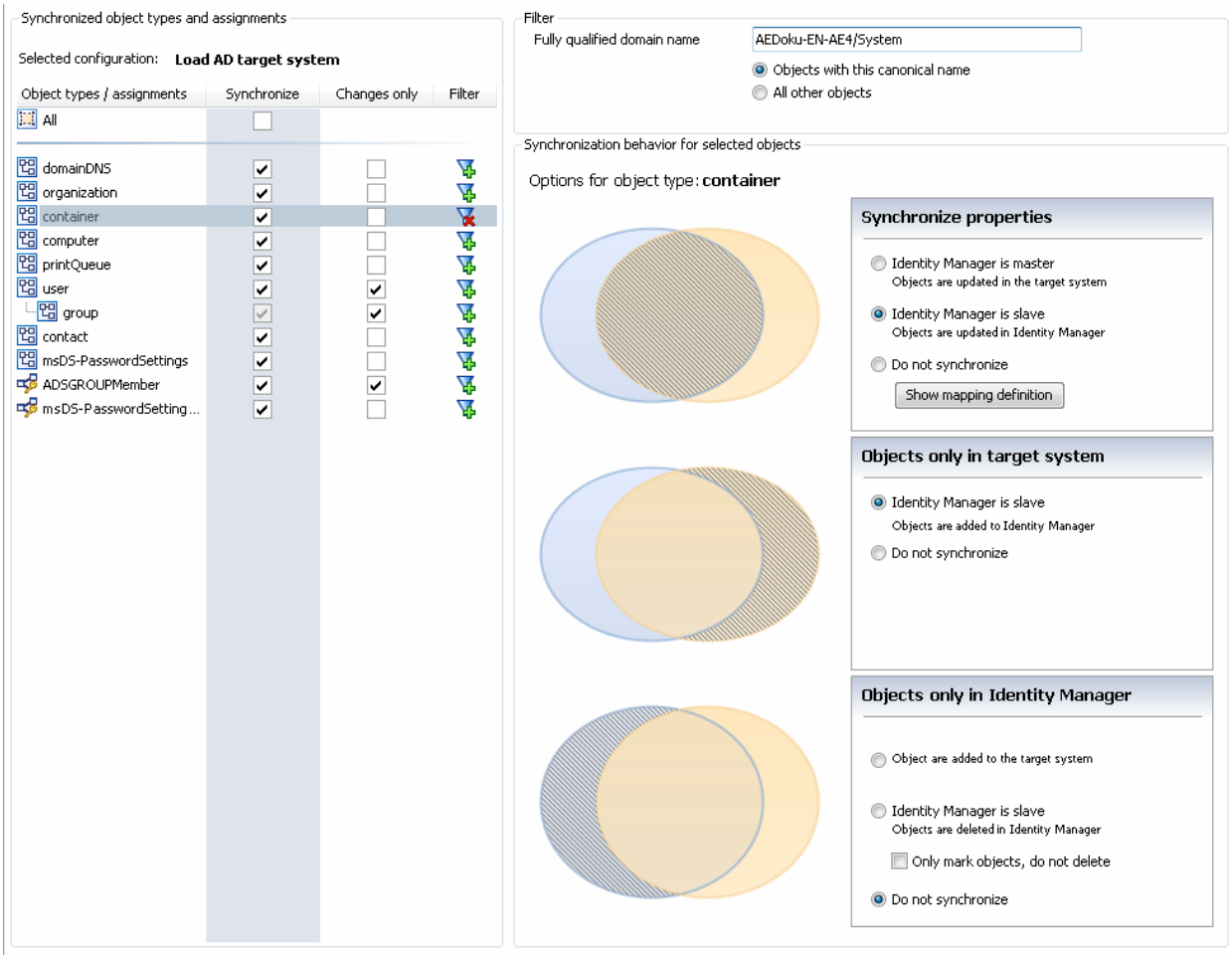

Additional settings
Option
Synchronize
Synchronize Active Directory system containers
Synchronize Active Directory system containers with advanced features
Synchronize Active Directory printer objects
Create hardware objects for imported printer objects automatically
Exclude Remote Access Service (RAS) property from synchronization
Exclude Terminal Service properties from synchronization
Write operating system and hardware installation type into 'description' p...
Also look for group members in following domains (delimit NetBios name...

Refer to the appropriate chapter for the different option in each target system: Special features of Active Directory Domain Synchronization Configuration on page 217, Special Features of Client Synchronization Configuration on page 358.

Object Type, Assignment and Synchronization Behavior

Specify which target system objects and assignment should be synchronized on the <Synchronization> tab. Define a data master for each object type/assignment and determine the behavior of the object property synchronization.

Select Object Types and Assignments



Synchronized Object Types and Assignments

In the <Synchronized object types and assignments> pane, select the object types and assignments that are going to synchronized. The object types and assignments are displayed on the form in the order they are going to be synchronized. The order is taken from the mapping rule.

The <Selected configuration> is the name of the synchronization configuration that you are currently working on. Specify which properties should be synchronized for each target system object and assignment. You can chose between the following options:

- Synchronization
  Selected object types are sychronized.

- Changes only
  Only objects taht have changed since the last synchronization are synchronized.
  See section How to Speed up Synchronization on page 174 for more detailed information.

- Filter
  Use the buttons to add or delete a filter for the object type/assignment. Apply the filters to limit which objects belonging to the selected object type/assignment should be synchronized. Read the section Filter on page 169 about the functionality of filters.

Set the option <All> on the <Synchonrization> tab to select all object types and assignments for synchronization.

In order to edit the sychronization behavior of an object type/assignment, mark the required line with the mouse. This display the currently specified synchronization behavior for the object type in the <Synchronization behavior for selected objects> pane. This can be modified here.

By selecting mulitple lines you can specify the same sychronization behavior for several object types. To do this, mark the affected object types/assignments with the mous. If you want to select all the object types/assignments set the <All> option with the mouse. This marks all object types/assignments. Fix the synchronization behavior for all marked object types/assignment by selecting the options in the <Synchronization behavior for selected objects> pane.

Filter

The <Filter> view is only shown if a filter is defined for an object type. Use the filter to limit synchronization to objects with canonical names given in the filter.

- Canonical name
  Enter a fully qualified domain name for the object that should be treated as a special case by the synchronization.
  The fully qualified name is formatted differently in each target sytem. For example, in Active Directory it is made up from the names of the domain, the container and parent container; in SAP R/3 from the names of the system, the client and object type.

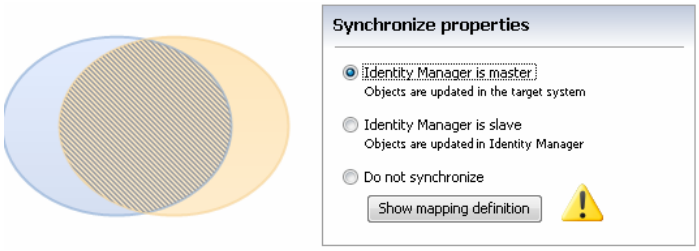
- Objects with this canonical name
  All objects whose canonical name begins with the given canonical name are synchronized. E.g.: all Active Directory containers whose canonical name begins with ”AEDoku-EN.AE4/System“. Only the Active Directory container ”System“ from the domain ”AEDoku-EN“ and all child Active Directory containers are synchronized.

- All other objects
  All other objects whose canonical name does not begin with the given canonical name are synchronized.
  E..g: all Active Directory containers which canonical name does not begin with ”AEDoku-EN.AE4/System“. The Active Directory container ”System“ from the domain ”AEDoku-EN“ and all child Active Directory containers are not synchronized. All other Active Directory containers are synchonized.

Synchronization Behavior for Selected Objects

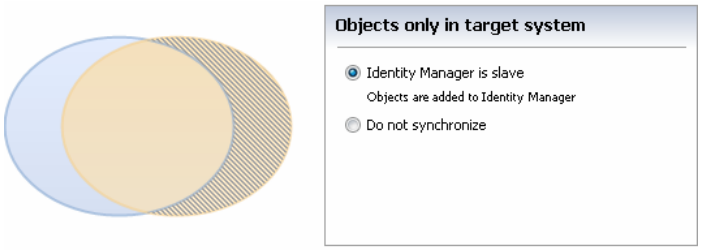
Use this pane to specify how sychronization objects should be treated during synchronization.

Synchronization of Properties


Synchronize properties
Identity Manager is master
Objects are updated in the target system
Identity Manager is slave
Objects are updated in Identity Manager
Do not synchronize
Show mapping definition

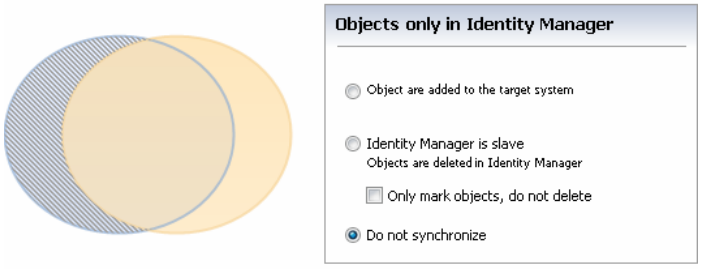
Object properties are synchronized for objects that are both in the Identity Manager database and the target system. Specify whether Identity Manager or the target system is the data master. Use the <Do not synchronize> option to stop object properties being synchronized.
The <Show mapping definition> button provides you with information about how each object property from the target system is mapped to the Identity Manager data model. You can edit this mapping. Read section How to Define a Mapping on page 175 for more information.

Objects on Exist in Target System



Specify whether objects that are only present in the target system are transfered to the Identity Manager database or not synchronized.

Objects Only in Identity Manager


Objects only in Identity Manager
Object are added to the target system
Identity Manager is slave
Objects are deleted in Identity Manager
Only mark objects, do not delete
Do not synchronize

Specify whether obejcts that only exist in Identity Manager should be transfered to the target system or deleted in the Identity Manager database. Use the <Do not synchronize> option to stop the objects being synchronized.

If you enable the option <Only mark objects, do not delete>, objects that do not exist in Identity Manager are labeled with the status ”Outstanding“. You can decide later whether these objects should be deleted from the database. If the option is not enabled, the objects are deleted immediately. See section Synchronization Analysis on page 176 about how to post-process objects with the status ”Outstanding“.

Affects of the Master Definition

Synchronization behavior should be made clearer by the following example.

Initial situation:

- There are user accounts in the database and in the target system with the properties ”key“ (for unique identification), ”name“, ”firstname“ and ”location“. There is also another property status (”S“) in the database.
- The user account property ”location“ has different values in the database and in the target system.
- There are user accounts in the database that are not in the target system.
- There are user accounts in the target system that are not in the database.

The differences in synchronization behavior are described using two possible master definitions. You can specify the master definition for each object type and each assignment separately and therefore combine the master definition in any way. How you can post-process synchronization objects is also defined. You can find further details in section Synchronization Analysis on page 176.

Target System is Master

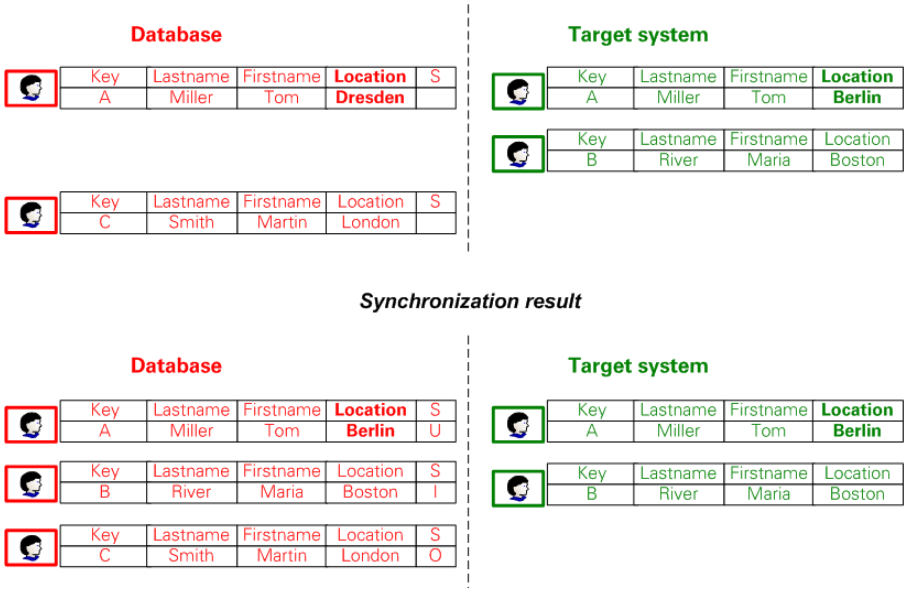
The following options are marked for synchronization behavior.

Synchronizing properties:	<Identity Manager is slave>
Objects only exist in the target system:	<Identity Manager is slave>
Objects only exist in the Identity Manager:	<Identity Manager is slave> <Objects only marked and not deleted>

Synchronization is solely in the direction of the target system. After synchronization, all target system user accounts exist in the database. New user accounts are marked with the status ”I“ (Inserted). No new user accounts are added to the target system. User account that only exist in that database are marked with the status ”O“ (Outstanding) because the option <Only mark objects and not delete> is

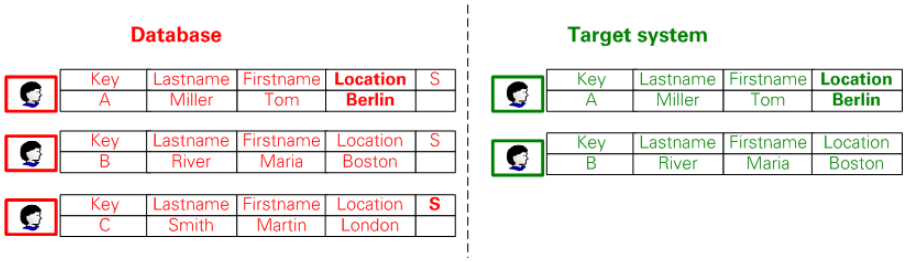
checked. Properties of existing user account are updated in the database and affected user accounts are marked with the status ”U“ (Updated).

System Behavior if Target System is Master

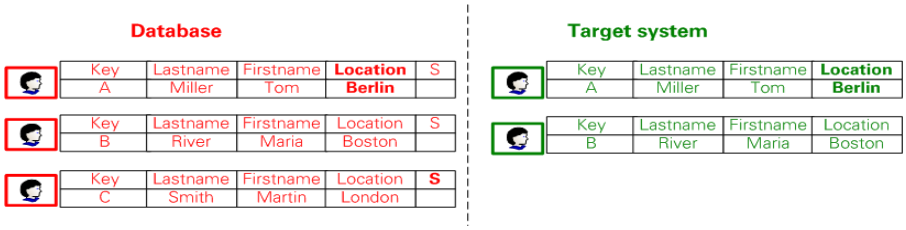


The following operations are permitted to post-process the marked user accounts:

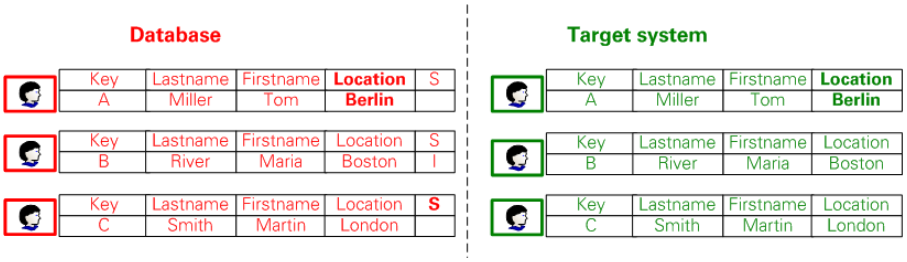
- Reset status
  The ”Status“ label is deleted in the database.



- Delete
  User accounts marked with the status ”O“ are deleted fromthe database.



- Publish
  User accounts marked with the status are added to the target system. The label is removed afterwards in the database.



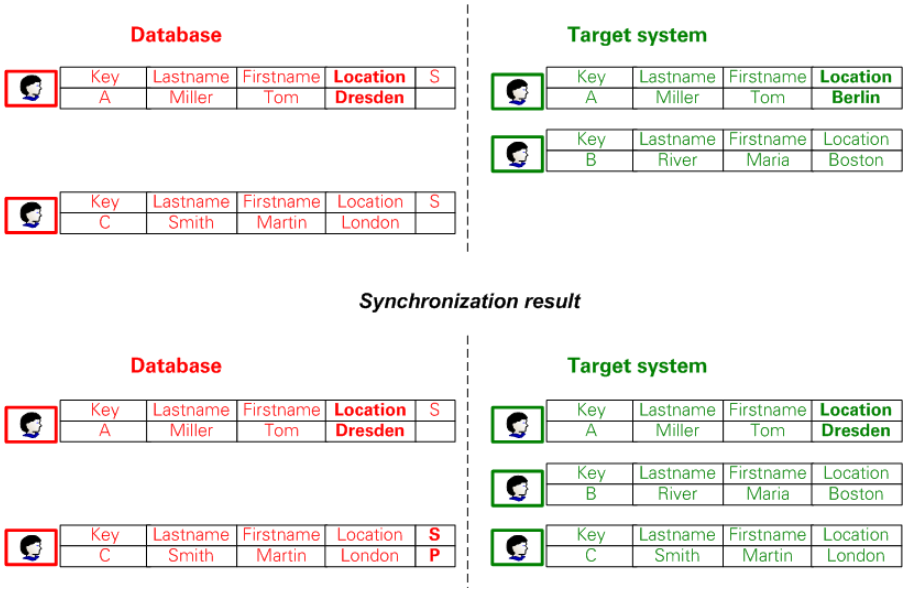
Identity Manager is Master

Following options are marked for synchronization behavior.

Synchronizing properties:	<Identity Manager is Master>
Objects only exist in the target system:	<No synchronization>
Objects only exist in the Identity Manager:	<Identity Manager is Master>

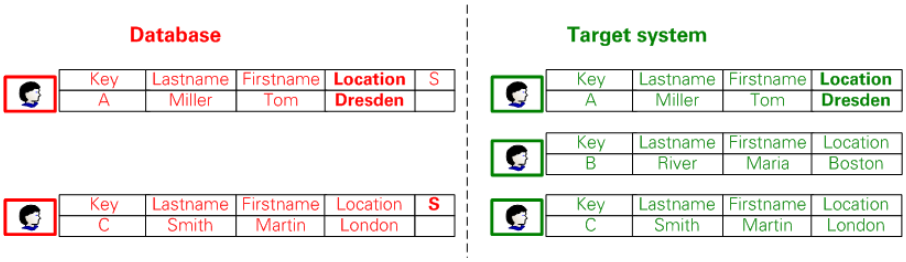
Synchronization in solely in the direction of the database. Properties of existing user accounts are updated in the target system. New user accounts are marked with the status ”P“ (Published“ and added to the target system. No new user accounts are added to the database.

System Behavior if Identity Manager is Master

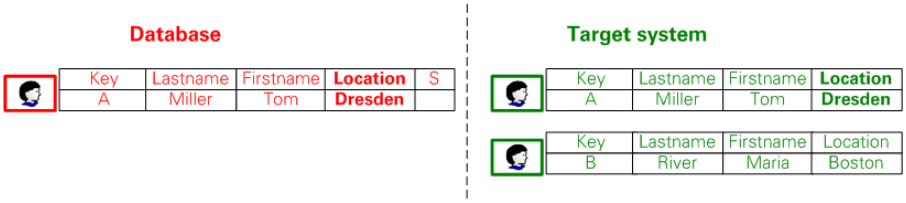


The following operations are permitted to post-process the marked user accounts:

- Reset status
  The "Status" label is deleted in the database.



- Undo and delete
  User accounts marked with the status "P" are deleted in the database and in the target system.



How to Speed up Synchronization

During synchronization all objects to be synchronized are loaded individually. Because this procedure can be time consuming in certain circumsances, objects that have not changed since the last synchronization can be excluded.

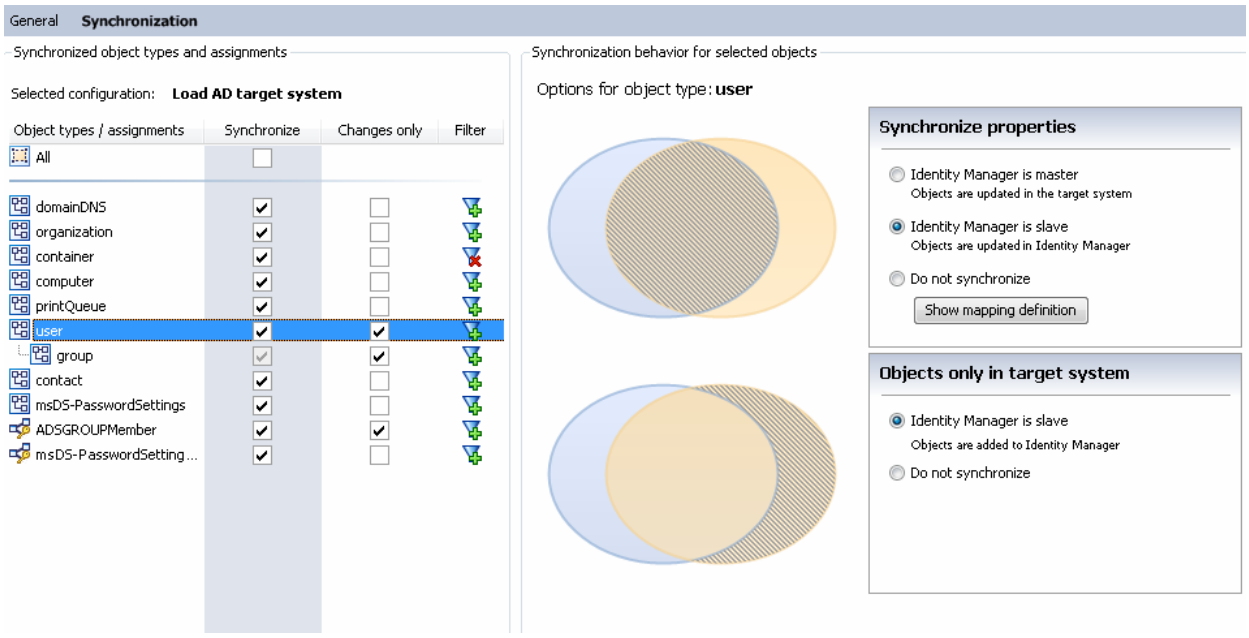
Each target system object contains data about its last modification. Each synchronization saves this change data in the Identity Manager database. The change data is also saved with the synchronization configuration. When the next synchronization in run the target system object change data is compared to the change data saved on the synchronization configuration. Only those objects from the target system whose change data is newer than the changed data in the Identity Manager database are synchronized. And only those objects from the Identity Manager database whose change data differs from the change data in the target system are transfered to the target system. This prevents objects that have not changed since the last synchronization from being updated. This limits the number of synchronization objects and speeds up synchronization.

Change Data for Acceleration per Target System Synchronization

TARGET SYSTEM	CHANGE DATA ON SYNCHRONIZATION OBJECT	CHANGE DATA IN SYNCHRONIZATION CONFIGURATION	COMMENT
Active Directory	Update Sequence Number (USN)	Highest rootDSE USN that can be determined for a domain controller.	
Lotus Notes	Update Sequence Number (USN)	Last synchronization date for domain	
SAP R/3	TRDAT	Last synchronization date for client	
LDAP	Change date in LDAP	contextCSN (ChangeSequenceNumber)	If the contextCSN cannot be found, Identity Manager creates its own time stamp.

Specify synchronization behavior for objects that only exist in the target system and for object properties.

Configuring Synchronization Acceleration



You can be assured that all all objects are synchronized that have been changed since the last synchronization due to the change data that is saved with the synchronization configuration. If you add a new object type to the synchronization configuration, then objects of this type that have change data older that of the synchronization configuration are not synchronized. Therefore, you have to run a full synch of all objects first. This updates the change data for all synchronization objects in the Identity Manager database.

How to Define a Mapping

Tool: Manager

Once the target system schema and the mapping rule have been read into the Identity Manager database you can view the mapping rule and edit it. Mapping rules can be modified for each part of n the target system. Only one mapping rule can be defined for each target system domain. Find out how to load the schema and mapping file into Identity Manager by reading section Loading Target System Schema and Mapping Rules on page 163.

You have two ways of starting the mapping editor:

1. Run the <Define mapping> task for this target system domain.
   The target system schema, synchronization object types and assignments and the database schema is displayed in the Mapping Editor.

2. Use the <Show mapping> button on the <Synchronization> tab of the synchronization configuration for an object type.
   The Mapping Editor also displays the map of the selected object type in the target system schema and in the database schema. You can also see how the object properties of the selected object type are mapped in the target system and in Identity Manager.

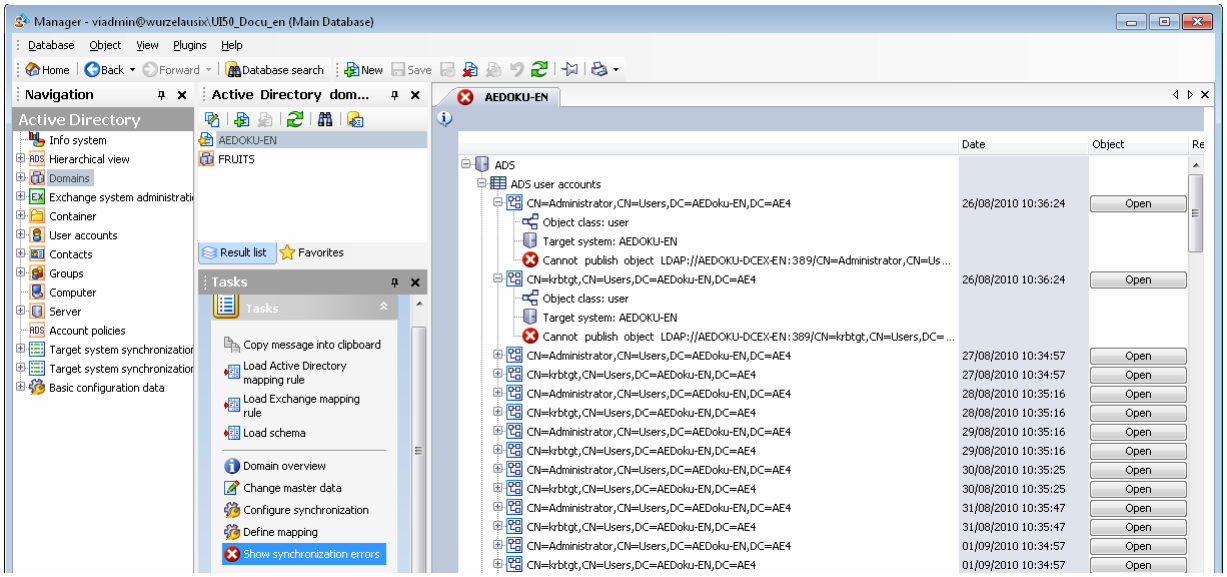
You can find out how to edit mapping rules with the Mapping Editor in section Customizing Mapping rules on page 180.

Logging Synchronization Errors

Tool: Identity Manager with application role <Target System>\<Target system manager>; Manager

Identity Manager logs activities and result of process components during synchronization. Objects that cause an error during synchronization are loaded into Identity Manager and logged. Change information is also update for these objects on each synchronization. These objects can be displayed and edited with Identity Manager tools. To do this, run the task <Show synchronization errors> on this target system domain.

Show Synchronization Errors



All the database tables with synchronization errors are listed on the form. The defined name, the object class, the target system domain, a detailed error description and the time of synchronization are displayed for each incorrect object. You can show details of each object's error in a separate window by using the <Open> button.

You may copy the error message for each object in to the clipboard for further processing. For this, mark the incorrect object (the defined name) and run the task <Copy message into clipboard>.

Every incorrect object appears only once in the list. If an error reoccurs on an object at the next synchronization, the error message is updated in the list. Old entries about incorrect objects are deleted. Identity Manager also tries to consolidate the incorrect objects after synchronization. If an object can then be synchronized successfully, the corresponding entry in the error list is deleted.

Use the <Remove> button to delete errors from the list.

Synchronization Analysis

Tools: Identity Manager with application role <Target systems>\<Target system managers>; Manager

During synchronization objects are marked with a label with a status and date format. The date respresents the time and date that an object was last synchronized.

Permitted status' are:

- Inserted
  This status labels objects that are inserted into the database during synchronization.

- Updated
  This status labels objects that already exist in the database before synchronization but whose properties are updated by a synchronization.

- Published
  Objects that already exist in the database but are not found in the target system are labeled with this status during synchronization with manual restore. These objects are added to the target system during synchronization.

- Outstanding
  Objects that already exist in the database but are not found in the target system are labeled with this status during synchronization with manual restore. These objects are not added to the target system during synchronization.

Objects that are labeled with the status "Outstanding" cannot be edited until the status is ultimately clarified.

Synchronisation Post Processing

Once synchronization has completed you can decide whether labeled objects require further handling. There are several options available to you for this. The label (status and time/date) is removed from the object after one of the operations has been executed. The status of the object determines which operations are permitted. The following operations are available for post-processing.

- Reset state
  The "Reset state" operation can be applied to all objects at any time. When this operation is carried out all the labels (state and date) are removed from the selected objects. A follow up synchronization in restore mode determines the new delta set and marks the objects found.

- Publish
  The operation "publish" ensures that the selected objects are added to the target system environment. The user account password is reset by publishing if user accounts are being dealt with.

- Undo
  The "undo" operation removes objects and dependencies that have already been added to the target system environment. The objects and dependencies are deleted from the target system and the database.

- Delete
  The "delete" operation deletes all the selected objects from the database.

The differences between the basic table objects such as the tables ”ADSAccount“ and objects in the reference tables (Many-to-many tables or ”Total” tables) such as the table ”ADSAccountInADSGroup“ ot the table ”ADSAccountInADSGroupTotal“ are taken into account.

Permitted Operations on Objects in the Base Table

OPERATION	STATE OF IDENTITFIED OBJECT			
	INSERTED („I“)	UPDATED („U“)	OUTSTANDING (”O“)	PUBLISHED (”P“)
Reset state	x	x	x	x
Undo	-	-	-	x
Publish	-	-	x	-
Delete	-	-	x	-

Permitted Operations on Many-to-many-Table Objects

OPERATION	STATE OF IDENTITFIED OBJECT			
	INSERTED („I“)	UPDATED („U“)	OUTSTANDING (”O“)	PUBLISHED (”P“)
Reset state	x	x	x	x
Undo	-	-	-	x
Publish	-	-	x	-
Delete	-	-	x	-

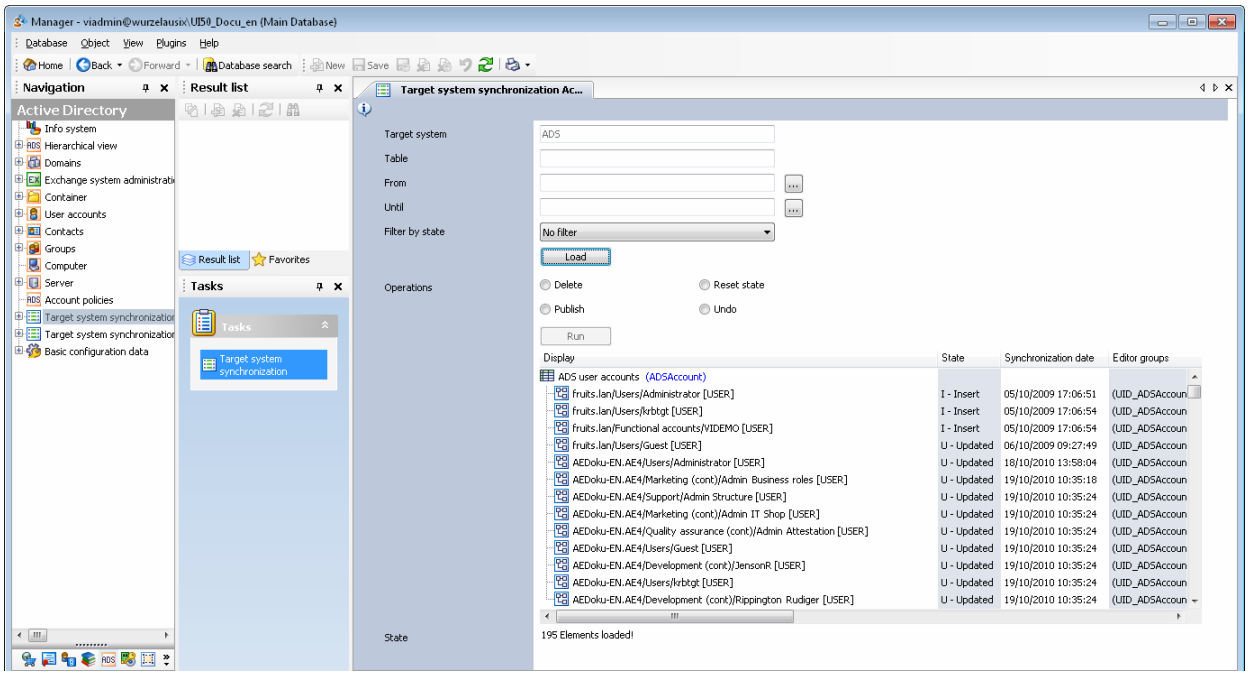
Permitted Operations on Objects in the ”Total“table

OPERATION	STATE OF IDENTITFIED OBJECT			
	INSERTED („I“)	UPDATED („U“)	OUTSTANDING (”O“)	PUBLISHED (”P“)
Reset state	x	x	x	x
Undo	-	-	-	-
Publish	-	-	x	-
Delete	-	-	-	-

Synchronization Data Display

Edit the marked objects in the category <target system>\<target system synchronization> . All synchronized database tables are listed for every target system.

Target System Synchronization using an SAP R/3 Example



The following information is displayed on the form for the synchronization objects:

- Target system
  Name of the target system whose synchronization objects are shown.

- Table
  Name of the database table whose synchronization objects are shown. The table can be selected in the navigation view and cannot be edited.

- From, 'til
  Limit the number of objects displayed by using the synchronization date. You set the time period using the buttons next to the input field.
  Use the <Load> button to reload the synchronization objects into the form according to the filter.

- Filter by status
  Limit the number of objects shown using the object status.
  Use the <Load> button to reload the synchronization objects into the form according to the filter.

- Operations
  Apply one of the operations <Delete>, <Reset status>, <Publish> or <Undo and delete> to the marked synchronization objects. Which operations can be applied to an object is described in section Synchronisation Post Processing on page 177.

- Status
  Additional status information, for example, the number of object loaded or object dependencies.

The middle part of the form displays the objects that have been found. They can also be edited here. To edit an object, select the required entry in the table. You can select more that one object with the same state (<shift> + <left mouse button> or <Ctrl> + <lift mouse button>) and edit them. The post processing operations that are allowed for objects are active.When an operation is selected a test report is created for dependent objects. In the report the table relations are evaluated and, depending on the restrictions, the dependencies are propogated in the test report. The selected operation can be started over the <Run> button.

Customizing Mapping rules

The functionality of Identity Manager Service covers specific process components for consolidating properties in the database with the target system. Mapping is carried out according to defined rules an specifications. A mapping rule embedded in the process component is used for the synchronization processes. Identity Manager allows extensions and customization of the mapping rules for synchronization processes.

The mapping rule not only applies to adding and changing an object in the database with subsequent publishing via Identity Manager Service but also to synchronization for clearing up data inconsistencies.

Basics for Customizing Mapping Rules

The mapping rules in process components correspond to a triple value set of the following kind:

Mapping Rule for Properties

PROPERTY IN TARGET SYSTEM	PROPERTY IN THE DATABASE	PARAMETER
P1	PX	PA
P2	PY	PB

If the properties are processed in an adhoc synchronization, the process component takes parameter ”PA“ and passes its value to the property ”P1“ in the target system. The database property ”PX“ is not relevant for synchronization

If the properties are processed during synchronization, the process component takes the target system property ”P1“ and passes its value to the database property ”PX“. The parameter ”PA“ is not relevant in this case.

Prerequisites for customizing mapping rules for process components are:

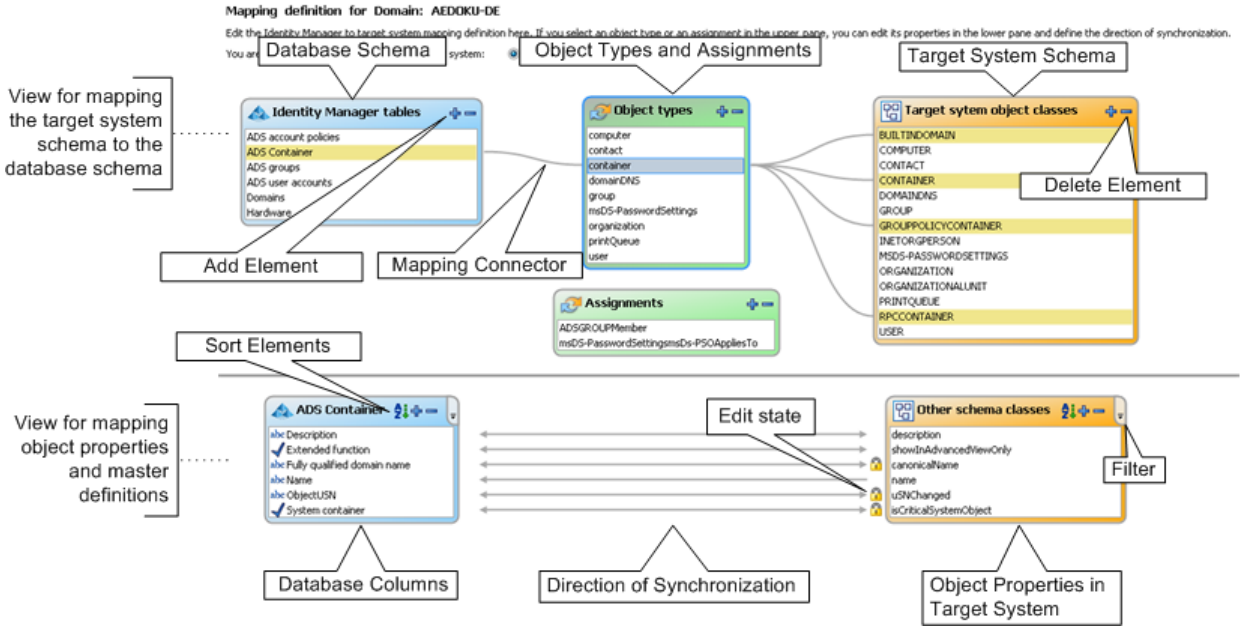
- Target system is loaded into Identity Manager
- Internal proess component mapping rules or one external mapping rule is loaded

You can find out how to load schema and mapping rules into the database in section Loading Target System Schema and Mapping Rules on page 163.

Mapping Editor Functions

Use the Mapping Editor to edit a mapping for target system synchronization with Identity Manager. This displays the target system schema, synchronization object type and assignments, the database schema as well as the object types in the target system and the Identity Manager database.

Mapping Editor



The Mapping Editor uses the following control elements to graphically represent the mapping.

View for displaying target system schema mapped to the database schema (upper pane):

- Target system schema
  This control element list all the object classes that are mapped in Identity Manager.

- Database schema control element
  This control element lists all the database tables that are connected to the target system schema.

- Object type and assignment control elements
  These control elements list all the object types and assignments for synchronization that establish a connection between the target system schema and the database schema. Use the <Add element> button to add object types or assignments. Use the <Delete element> button to remove object types or assignments.
  You can edit the properties by double-clicking on the properties of the selected object type or assignment.

- Mapping lines
  Mapping lines show which elements the target system object classes are mapped to in the database schema. Mark one object type/assignment with the mouse.
  Double-click on a mapping line to highlight it. Then you can delete the connection with via the context menu.

- Add element(s)
  Select additional object classes or database tables that you want to map from a drop-down menu.

- Delete element
  Deletes marked object classes or database tables from the mapping file.

View for mapping object properties and master definitions (lower pane):

- Target system properties
  This control element shows all the object properties of objects classes selected in the target system schema that are mapped in Identity Manager.

- Database columns
  This control element shows all columns of the database tables selected in the database schema that have a connection to target system properties.

- Add element(s)
  Select additional target system properties or database columns that you want to map from a drop-down menu.

- Delete element
  Deletes the marked target system property or database column from the mapping file.

- Sort elements
  Target system properties and database columns are listed in increasing alphabetical order.

- Filter
  Filters the target system properties or database columns to be displayed. There are four pre-defined filters there to help you.

All	Shows all elements
Master definition exists	Show all elements that have a master defined.
Target system is master	Displays all elements that have the target system defined as master.
Database is master	Displays all elements that have Identity Manager defined as master.

- Direction of synchronization
  Shows the master definition for the object type.

No master defined.

Database is master.
Empty database columns are not overwritten.

Target system is master.
Empty database column are not be overwritten.

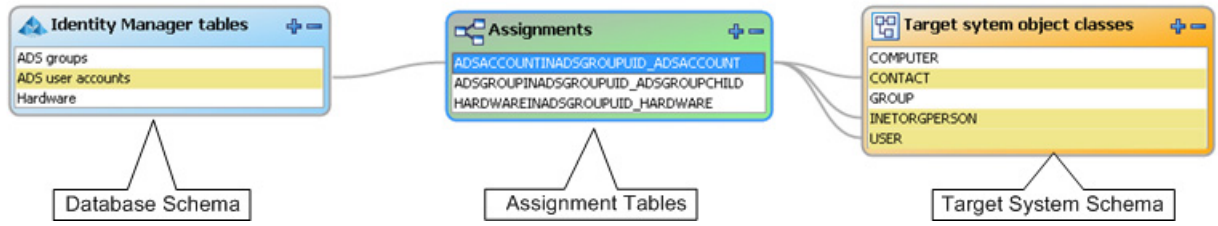
Target system is master.

You can change the master definition by double-clicking with the mouse.
Click the mouse once to mark the synchronization arrow. Using the context menu you can delete the connection or edit the column mapping.

- Editing status
  The symbol is displayed if the target system property or the database column may not be changed by synchronization.

The following control elements are shown for assignments in the object property and master definitions view.

Mapping Editor for Assignments



- Target system schema
  This control element lists the target system object classes that are mapped via the assignment that are marked in Identity Manager.

- Assignment tables
  This control element list the assignment tables that are connected to the target system schema via the marked assignments.

- Database schema
  This control element lists all the database tables that are taken as base tables in the assignment.

Editing a Mapping Rule

You can edit how target system object classes are mapped to database tables, object type properties and assignments, the column mapping and master definitions.

A complete mapping for an object type includes:

- Name of the object type
- Object class assigned to the target system
- Assigned database table
- Master definition at least for the compulsory columns of the assigned database table

A complete mapping for an assignment includes:

- Name of the assignment
- Object class assigned to the target system
- Assigned database table
- Assigned assignment table
- Target system object classes mapped to the assignment table

- Assigned base table

Objects are not or incorrectly synchronized if the mapping is not fully defined for an object type or an assignment.
Check whether the mapping is fully defined for all object types and assignments before saving the mapping rule.

Changes to the mapping rule are saved in the ”MappingInfo“ column and in also the mapping file stored in the target system domain. Any name and directory path can be chosen for the mapping file. However, it is recommended that you use the target system domain identifier and place the file in the Identity Manager Service installation directory on the synchronization server.

Syntax:

```
<Identifier>.XML
```

Example:

```
ADSDomain01.XML
```

If there is no mapping file, Identity Manager saves the mapping rule in its own mapping file. The file name is formatted as follows:

```
<Name of assembly file>.XML
```

Example:

```
ADSComponent.DLL.XML
```

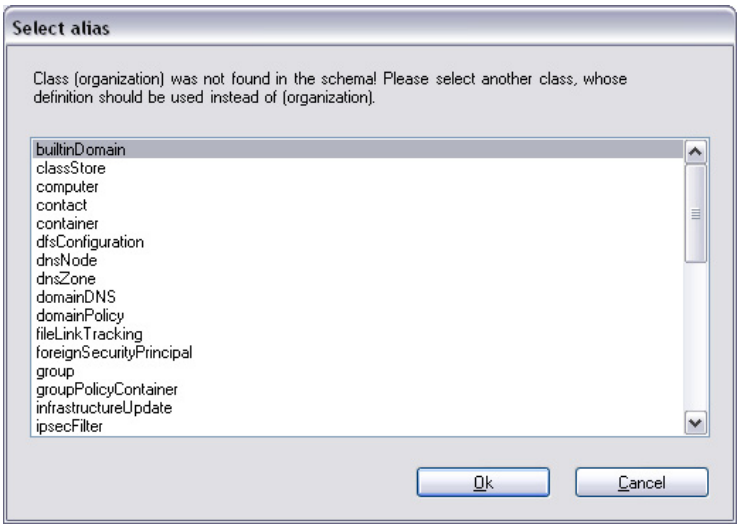
If this file does not exist, Identity Manager creates it on the synchronization server when the mapping file is saved for the first time.

Each process function of the target system specific process components has an optional parameter ”MappingDefinition“ which allocated a valid mapping file. This parameter is enabled in the default Identity Manager installation.

If you edit a mapping file with another editor (in a local copy for example), load the file with the software loader into the database. The file is automatically distributed to the synchronization server by automatic software update. You can find details of the automatic software update in section Automatic Job Server Updating on page 89.

If you load the mapping rule from an external mapping file, take note of the following:
If there are object classes in the mapping file that are not in the target system, you are prompted to assign object classes to be used from the target system schema for these object classes.

Assign Missing Object Classes



- Select an object class from the list. Confirm selection with the <OK> button.
- If you do not want to assign a new object class, close the window with the <Cancel> button. The missing object classes are ignored by the synchronization.
- Other missing object classes can be edited.

Mapping Target System Schema to the Database Schema

In the upper part of you see how the object types, assignments, database tables are mapped to object classes in the target system. To do this, mark an object class, an object type or an assignment. If you want to find out which object types or assignments are used to map the object classes in the database schema, mark a database table.

You can change object class mappings to database tables. To do this, delete the existing mapping line and add a new one.

1. Mark a connection line.
2. Delete the selected line via the context menu.
3. Mark an object type or assignment.
4. Hold down the left mouse button and pull the new connection line from the selected object type or assignment to an object class or database table.

If you have customized the Identity Manager data model, the modification can be included in the synchronization. Proceed as follows:

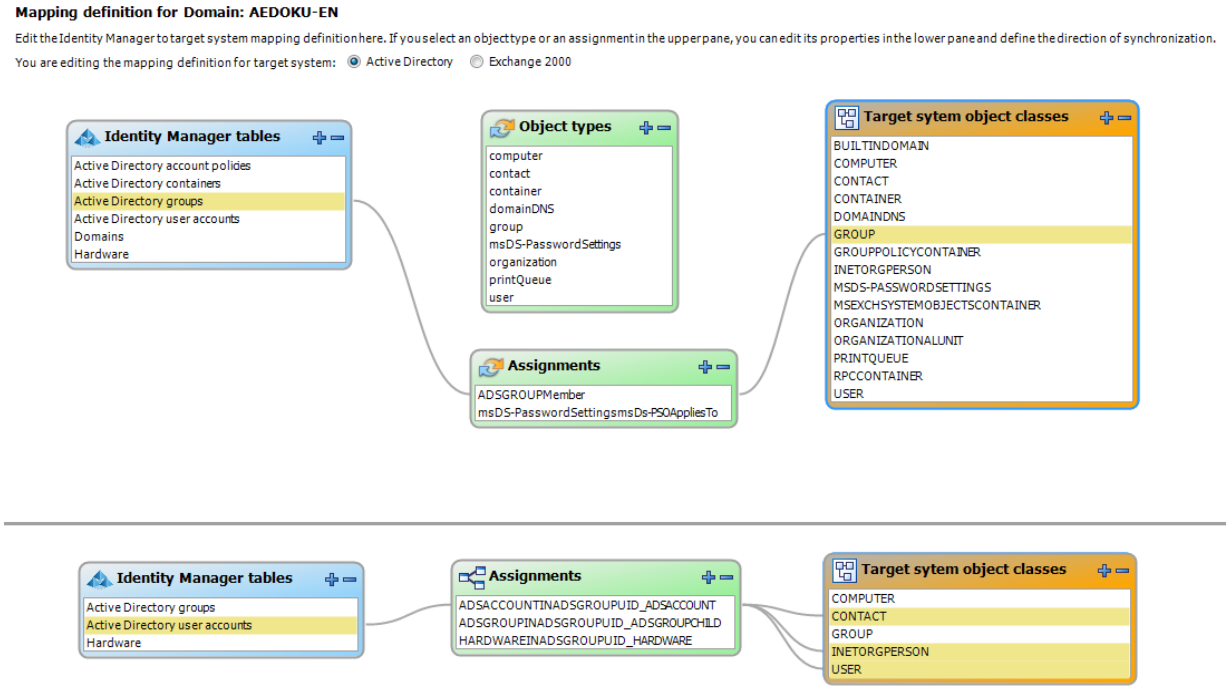
1. Add new tables and object classes via the <Add element> button in the mapping definition.
2. Add a new object type or assignment with the <Add element> button.
   Enter a unique ID for the object type or assignment in the <Key> field.

3. Hold down the left mouse button and pull the new connection line from the new object type or new assignment to a new database table.

Mapping Object Relations

Relations between target system object classes in Identity Manager are mapped used assignments. These relation are made in Identity Manager via assignment tables. To do this, mark an assignment in the upper pane of the mapping definition. The database table that is highlighted is part of the assignment table.

Mapping Object Relations



All assignment table that are written by the selected assignment are displayed in the lower pane of the mapping definition. For each assignment table, specify which database table - and therefore which object classes - are included in the assignment . If you mark an assignment table, the database table is highlighted that makes up the second part of this assignment table. At the same time you can see which target system object classes are mapped in the highlighted database table.

You can change object class mapping to assignment table by deleting the mapping lines from the context menu and adding new ones.

Adding elements to the Mapping Definition

The Mapping Editor control elements have an <Add element> button. You can use this button to add new elements into the mapping definition. If you add a new object type or a new assignment, define all the elements that are required for a complete mapping definition (see section Editing a Mapping Rule on page 183). If you add a custom database table to the mapping, you need to at least define the column mapping for the mandatory columns in this table.

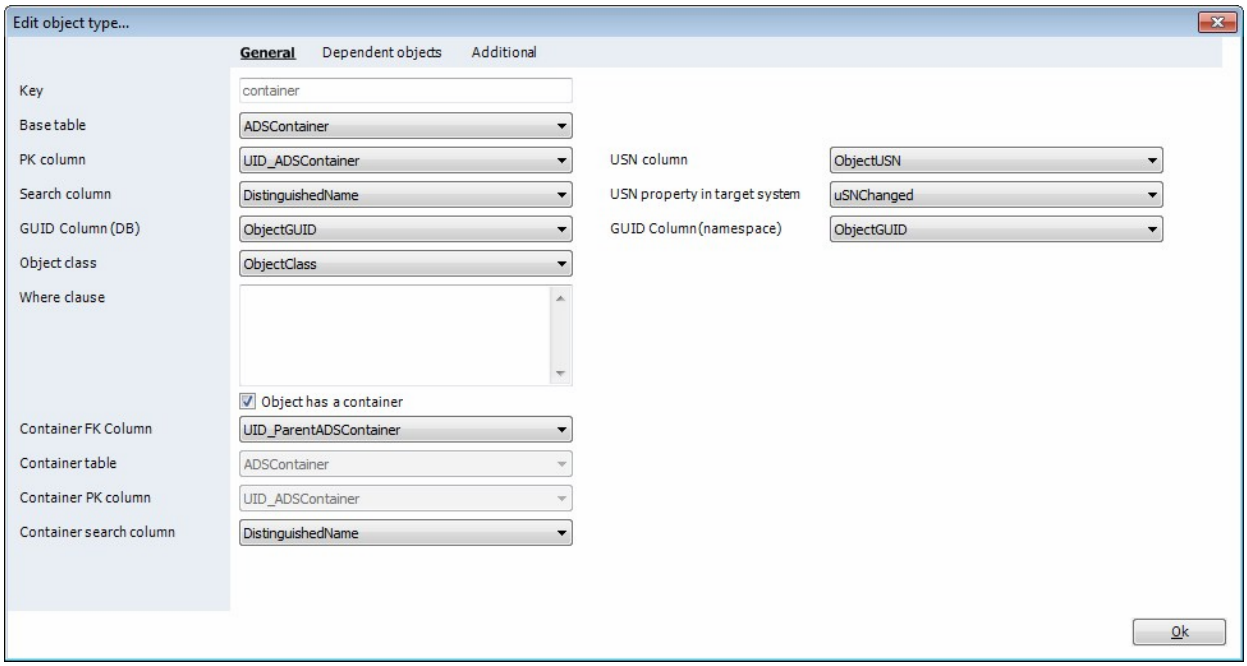
Deleting Elements from the Mapping Definition

The Mapping Editor control elements have a <Delete element> button. You can use this button to delete the chosen element from the mapping definition. Check that the mapping definition is still complete all the elements that were connected with the deleted element (see section Editing a Mapping Rule on page 183). Remove all other elements that are no longer required or assign other element to the mapping definition.

Editing Object Types

By double-clicking on an object type you can edit the object type properties.

Editing Object Types



Enter the following data for an object type:

- Key
  Unique identifier for the object type
- Base table
  The object type is mapped to this database table.
- PK column
  Table column in the base table that contains the primary key.
- Search column
  Table column in the base table that contains the X500-DN or a unique search string. In Lotus Notes it is ”Fullname1st“.
- GUID column (database)
  Table column in the base table that contains the object GUID for the sychronization objects.

- Object class
  Table column in the base table used to determine the object class. If this field is empty, the target sytem object class is used.

- Where clause
  Where clause, for limiting the number of synchronization objects.

- Object has a container
  If this option is enabled, the table is linked to the hierarchical structure of the target system. More object properties are displayed.

- Container FK column
  Table column in the base table that contains the foreign key for the parent container.

- Container table
  Database table that contains the target system container.

- Container PK column
  Table column in the container table that contains the primary key for the container.

- Container search column
  Search column for the container
  Table column in the container table that contains the X500-DN or a unique search string.

- USN column
  Table column in the base table that contains the USN data from the last synchronization. This input field is only applies to the target systems Active Directory and Lotus Notes. For more information see section How to Speed up Synchronization on page 174.

- USN property in target system
  Object property in target system that keeps USN data available. For more information see section How to Speed up Synchronization on page 174.

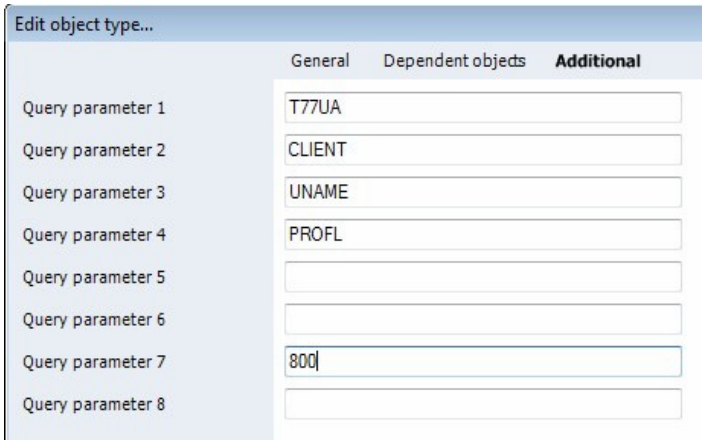
- GUID column (target system)
  Object property in target system that contains the object GUID for the synchronization object.

Formulating the Mapping Definition as an SQL Query

You can detemine target system properties for target systems that use an SQL database as a basis via SQL queries and synchronize directly with a database table. Add a new object type for this and connect

it with a database table and with the object class ”SQL“. Open the property window for this object type. You can enter all the parameters required for the SQL query on the <Additional> tab.

Entering SQL Query Parameters



Enter the following values for the SQL query:

- Query parameter 1
  Target system table whose data should be synchronized.
- Query parameter 2 ... Query parameter 6
  Target system columns whose values should be synchronized.
- Query parameter 7
  Limiting condition for columns in query parameter 2
- Query parameter 8
  Limiting condition for columns in query parameter 3

Identity Manager formats the following SQL query on an SAP system using the query parameters in the example show in the graphic above:

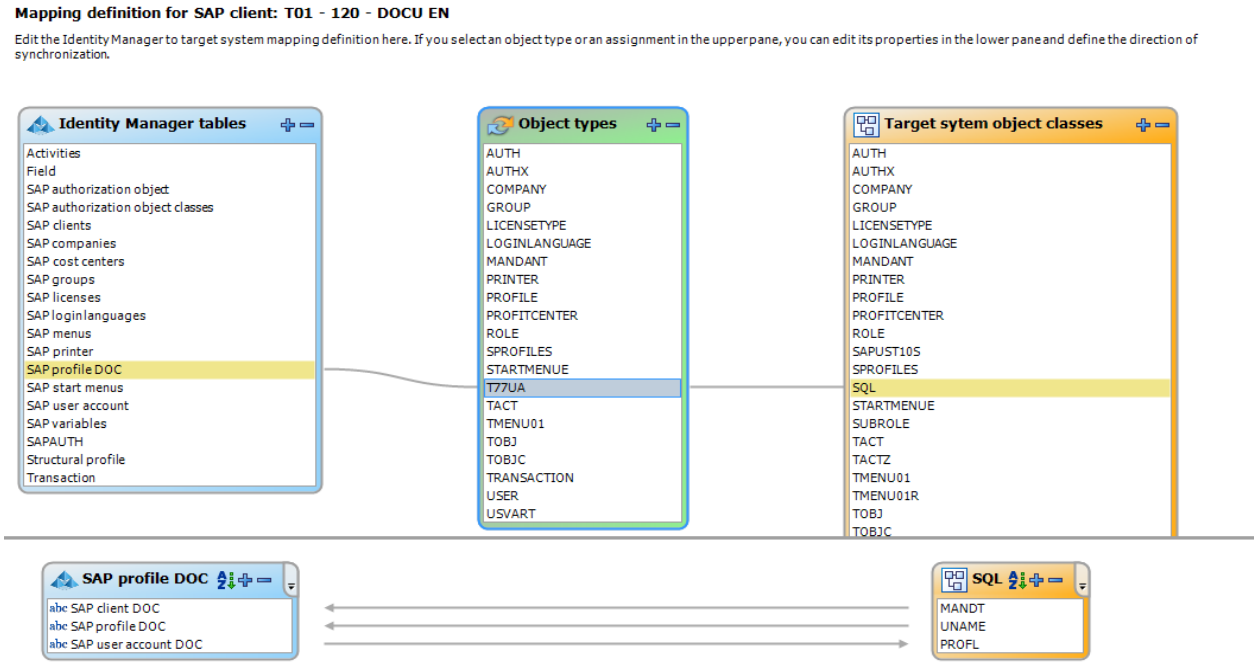
```
select MANDT, UNAME, PROFL from T77UA where MANDT = ´800´
```

Define the column mapping for the query parameter. Proceed as follows:

1. Add target system properties
   See section Adding elements to the Mapping Definition on page 186
2. Add database columns
   See section Adding elements to the Mapping Definition on page 186
3. Specify data master
   See section Specifying the Data Master for Object Properties on page 192
4. Post process column mapping if required
   See section Modifying the Column Mapping on page 192

The complete mapping definition for an SQL query is displayed as follows in the mapping editor:

SQL Query Mapping Definition

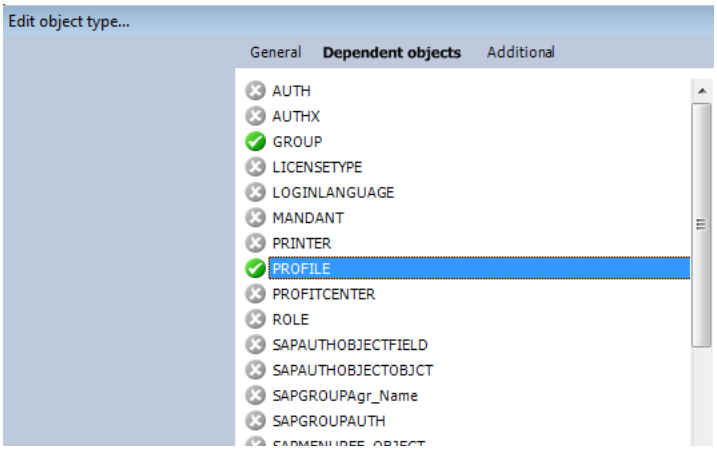


Defining Dependencies

Dependencies can be defined for object types and assignments from other object types or assignments. Object types or assignments marked as dependent represent a direct prerequisite for synchronizing an object type or an assignment. This ensures that certain objects are only synchronized if the dependent object has been synchronized

Define dependencies in the properties window of an object type or an assignement on the <Dependent objects> tab.

Specifying Dependencies



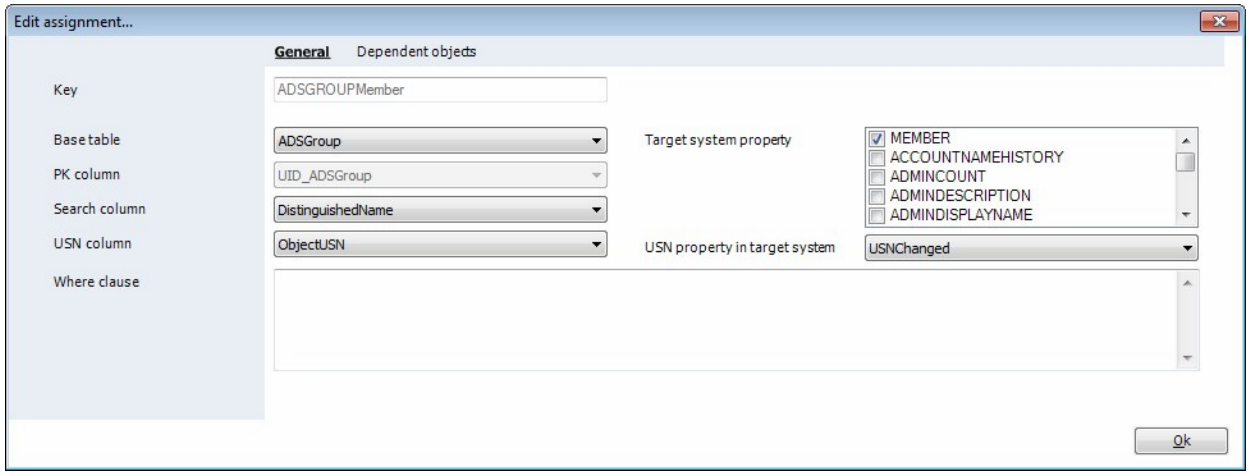
Assign the objects type and assignments that are prerequisites for synchronization of the selected object type or assignment. Use the <OK> button to save the assignment. The assigned objects types and

assignments are shown as dependent in the synchronization configuration. For more information see section Object Type, Assignment and Synchronization Behavior on page 168.

Editing Assignments

By double-clicking on an assignment you can edit its properties.

Edit Assignment



Enter the following data for an assignment:

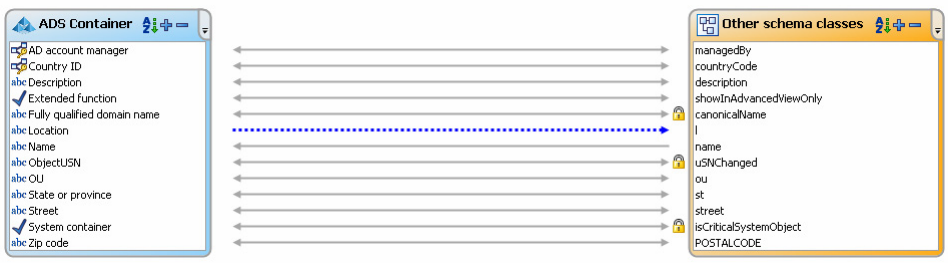
- Key
  Unique identifier for the assigment
- Base table
  The assignment is mapped to this database table.
  Forms part of the assignment tables that are written due to this assignment.
- PK column
  Table column in the base table that contains the primary key.
- Search column
  Table column in the base table that contains the X500-DN or a unique search string. In Lotus Notes it is ”Fullname1st“.
- USN column
  Table column in the base table that contains the USN data from the last synchronization. This input field is only applies to the target systems Active Directory and Lotus Notes. For more information see section How to Speed up Synchronization on page 174.
- GUID column (target system)
  Object property in target system that contains the object GUID for the synchronization object.
- Where clause
  Where clause, for limiting the number of synchronization objects.
- Target system property
  Property of the target system object class used for setting up the assignment.

- USN property in target system
  Object property in target system that keeps USN data available. For more information see section How to Speed up Synchronization on page 174.

Specifying the Data Master for Object Properties

You have the option to specify whether the database or the target system is the data master for the mapping the data for each object property. To do this you mark an object type in the upper mapping pane. The target system properties and the database columns as well as the direction of synchronization are displayed in the lower pane for the selected object.

Specifying the Data Master



By double-clicking on the synchronization direction arrow you can change the data master. To specify a new direction for synchronization, mark a target system property and click and old the leftmouse button and drag a connection to the database column (or vice versa). This removes the existing synchronization direction arrow and redisplays it.

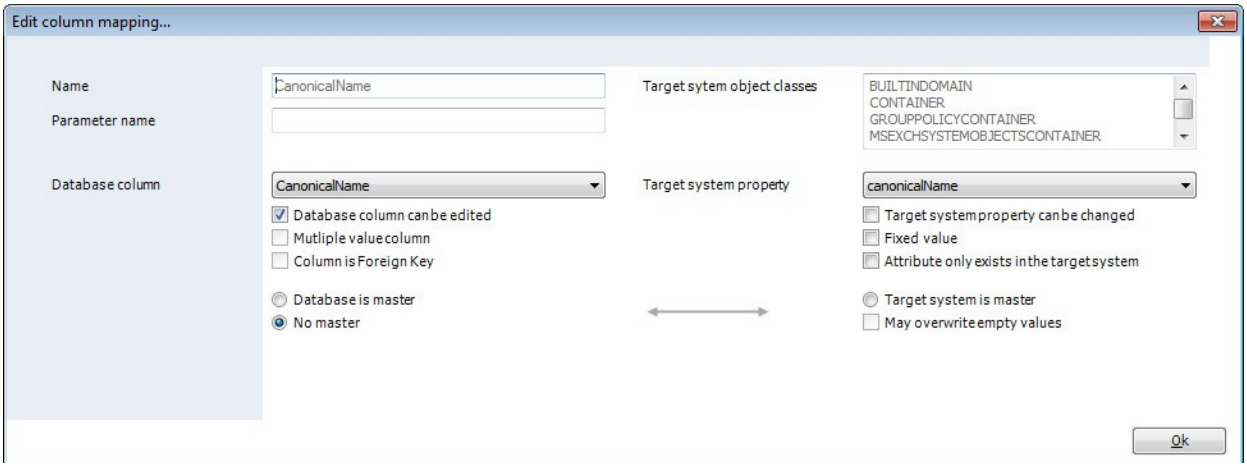
Delete a master definition using the synchronization direction context menu. Run the command <Delete selected connection> to do this.

Changes to the master definition are saved separately in an XML structure in Many-to-many the database. You can view and edit this XML structure on the target system domain's master data form on the <Synchronization> tab, input field <Attribute synch. definition>.

Modifying the Column Mapping

You can use the synchronization direction context menu to modify the mapping definition for an object property. To do this, run the task <Edit column mappings...> from the menu. You can also open the window by double-clicking on a database column or a target system property.

Modifying the Column Mapping



Enter the following details for the object property mapping definition:

- Name
  Unique identifier for the column mapping
  This is preformatted automatically from the name of the database column when a new column mapping is added.

- Parameter name
  Name of the process parameter that is defined in the process component for modifications to this column.
  Changes to the parameter have to be maintained in all process steps that this parameter uses. See section Process Step Parameters on page 58 in the Process Orchestration Manual to find out how to edit a process parameter.

- Database column
  Name of the database column that target system property is mapped on.

- Database column can be edited
  If this option is set, changes to the target system property can be transfered to the database.

- Multiple value column
  If this option is set, the target system property is mapped to a MVP column (MultiValuedProperty).

- Column is foreign key
  If the option is enabled, the target system property is mapped to a foreign key column.

- Target system object classes
  List of all object classes that belong to the target system property.

- Target system property
  Name of the object property in the target system that is mapped to the database column.

- Target system property can be changed
  If this option is set, changes to the database column can be transfered to the target system.

- Fixed value
  If this option is set, a fixed value is written to the database column. Enter the fixed value in the input field, <Target system property>.

- Property only exists in the target system
  If this option is set, there is no database column that the target system property can be mapped to. The target system property can be derived from other Identity Manager data. Changes to this data are written into the target system during synchronization; a synchronization from the target system to Identity Manager does not take place.
  A database column corresponding to this target system property is written in the mapping definition whose name begins with ”_“.

- Database is master
  If this option is set, changes to the database column are written to the target system.

- No master
  If this option is set, there is no master defined. The master synchronization configuration definition is used for synchronizing.

- Target system is master
  If this option is set, changes to the target system property are written in the database.

- May overwrite empty values
  If this option is set, object properties that do not have a value in the database are copied from the target system. The option only applies if the database is defined as master. In the case of empty values the definition of the master no longer applies.
  The option can only be set if the option <Database is master> is set.

- Direction of Synchronization
  Is displayed with respect to the definition of the master.

Special Cases of Synchronization

The options <Database column can be changed> and <Target system property can be changed> show whether it is technically possible to update the appropriate object properties in the target system or in the database. These options have precidence over the master definition. That means:
If the option <Target system property can be changed> is not set, changes in the database column are not written to the target system even if the database is defined as master.

Target system properties that have the option <Property only exists in the target system> set are written to the target system during synchronization. However, these properties are not synchronized in the database.

Example:

If the ISO country code is set up via a FK relation on an Active Directory user account (table ADSAccount), then both the country abbreviation and the ISO country code from the table referenced by the foreign key, ”ADSCountryCode“, must be passed via update process steps. The country code is only required by synchronization to create the FK relation because the values in the table ”ADSCountryCode“ are preset.

Data node in the mapping file (XML structure):

```
<Data Name="SYNCIGNORESTHIS" NSColumn="c" UpdatableNS="True" DBColumn="_1"
UpdatableDB="False" IsFK="True" FKTable="ADSCountryCode"
FKColumn="Ident_ADSCountryCode" FKSearch="c" />
```

Database columns that have the option <Fixed value> set are assigned a fixed value during synchronization. This might be necessary, for example, when a database column is mandatory in Identity Manager but the object property does not exist in the target system.

Example:

In the LDAP target system, a user can be assigned different object classes. In Identity Manager a user should only be assigned one object class. This is the value that is written to the database during synchronization.

Data node in the mapping file (XML structure):

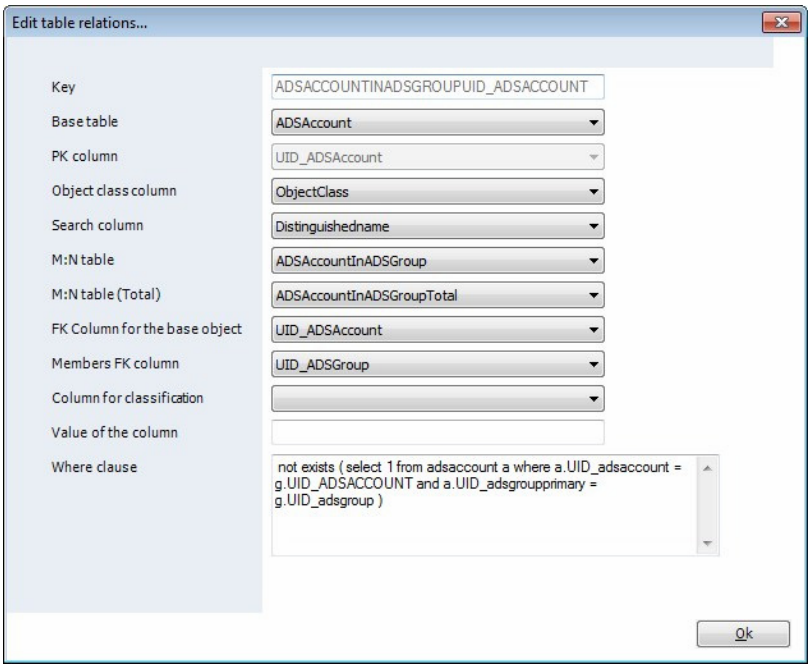
```
<Data Name="OBJECTCLASS" NSColumn="VALUE=INETORGPERSON"
UpdatableNS="False" DBColumn="ObjectClass" UpdatableDB="True"
IsFK="False" IsMVP="False" ParamsColumn="" IsMVP="False"/>
```

Editing Table Relations

By double-clicking on an assignment table you can edit its table relation. Specify which database table and database columns are a part of the assignment. You can reduce the number of synchronization ob-

jects if necessary by applying a where clause. To do this, mark an assignment in the upper pane of the mapping definition and select an assignment table in the lower pane.

Edit Table Relations



Enter the following data for table relations:

- Key
  Unique identifier for the relation
  By default, the name of the assignment table and the primary key column of the base table are used as identifier.

- Base table
  The table that is connection to the assignment in the lower pane of the mapping definition.

- PK column
  Name of the column in the base table that contains the primary key.

- Object class column
  Name of the column in the base table used by the object class to store the synchronization objects.

- Search column
  Table column in the base table that contains the X500-DN or a unique search string.

- Many-to-many table
  Name of the assignment table

- Many-to-many table (Total)
  Name of the associated total assignment table

- FK column for base object
  Name of the foreign key column in the assignment table that links to objects in the base table.

- Members FK column
  Name of the foreign key column in the assignment table that links to the objects in the connected table (table that is linked to the assignment in the upper pane of the mapping definition).

- Column for classification
  Column of an extended assignment table for classifying synchronization objects.
  Example: column ”NotesRestrictType“ in assignment table ”NotesserverRestrictGroup“.

- Column value
  Value that is entered in the column for classification.
  Example: ”AllowAccess“ in column ”NotesRestictType“

- Where clause
  Where clause, for limiting the number of synchronization objects.

Example of classification:

In the assignment table ”NotesServerRestrictGroup“ there are groups assigned to Notes servers with limited permissions. The type of restriction is stored in the extended property <NotesRestrictType>. During synchronization, groups with the target system property ”AllowAccess“ should be taken into account. Which target system objects should be synchronized with which assignment table is given in the mapping rule.

Synchronization Server Administration

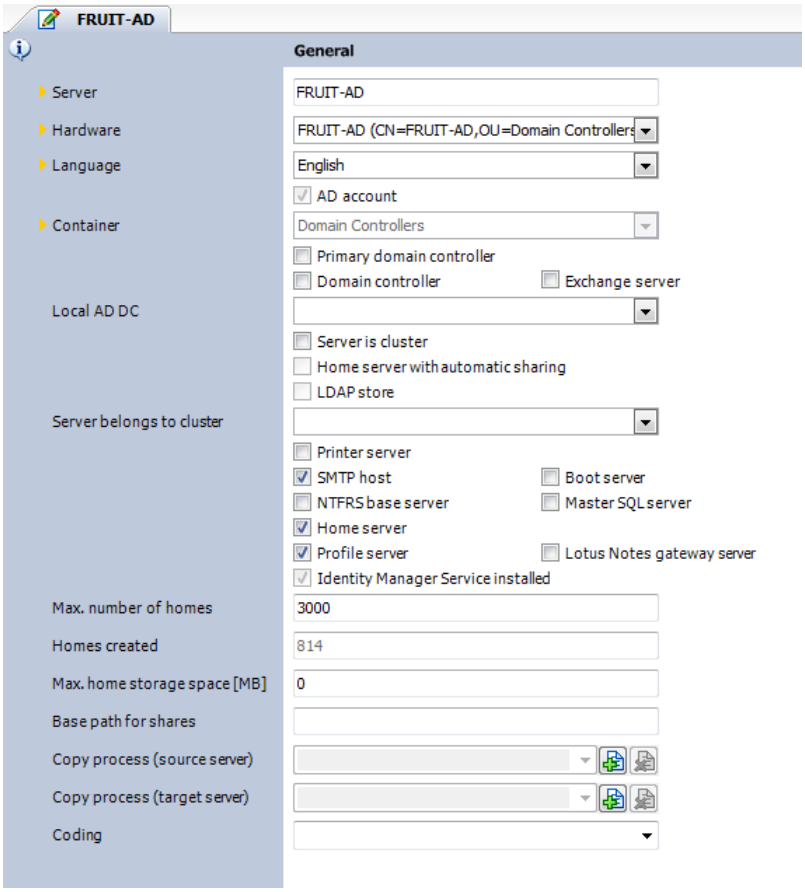
Tools: Manager; Identity Manager with applicaiton role <Target system>\<Target system managers>

A synchronization server must be installed and declared in the Identity Manager database so that the Identity Manager can execute a synchronization. Assign the synchonization servers to the synchronization base object (Active Directory domain, SAP system, LDAP domain, Notes domain) in the target system. There are several options available - depending on the target systems to be connected. For more information refer to sections Declaring the Active Directory Synchronization Server on page 205, Declaring the Synchronization Server on page 348, Declaring the Gateway Server on page 306 and Declaring the LDAP Synchronization Server on page 403.

You can enter other properties for the synchronization server. Open the synchronization server master data form to do this. You have several options available depending on the target system.

Active Directory:	category <Servers>
Microsoft Exchange:	category <Active Directory>\<Servers>
SAP R/3:	category <Basic configuration data>\<Servers>
Lotus Notes:	category <Basic configuration data>\<Servers>
LDAP:	category <Basic configuration data>\<Servers>

Editing Synchronization Server Properties



The following data is necessary for the synchronization server. This is already entered when the server is set up.

- Server
  Server name
  The server name is formed from the queue name for the corresponding Job server. The process steps are requested from the Job queue with exactly this name.

- Hardware
  Name of the hardware that the synhronization server is installed on.

- Language
  Language setting for the synchronization server.

The following properties may be necessary depending on the target system.

- Primary domain controller/domain controller
  Netlogon directories are automatically replicated by the Identity Manager Service between servers that are defined as domain controllers. Server that are not marked as domain controllers are treated as member servers.

- Exchange server
  Declare the server for synchronizing with Microsoft Exchange.

- Lotus Notes Gateway Server
  Declaring the gateway server is a prerequisite for synchronizing the Identity Manager with Lotus Notes.

- LDAP store
  Enable this option for the LDAP store server. Entering a server with LDAP store is the prerequisite for synchronizing between the LDAP directory and the Identity Manager database.

The following properties can be entered for a server:

- AD account

- Container
  Allocate the Active Directory container in which the server has a user account.

- Local AD DC
  You can enter a domain controller that is physically nearby for home servers, profile servers or exchange servers on a member server. If no server is entered the main AD synchronization server for the Active Directory domain is used.

- Cluster server
  If the server represents a cluster you must set the appropriate options. If the server belongs to the cluster, select it in the cluster list. The option <Server is cluster> and the selection <Server belongs to cluster> are mutually exclusive.

- Home server with automatic sharing
  Set this option for a Microsoft Home cluster that was installed according to Microsoft requirements. In this case the user‘s home directories are not added and shared through the Identity Manager but created automatically through the Cluster.

- Printer server
  This option is set if the server should server as a printer server.

- SMTP host
  Service mails can be sent by the Identity Manager Service on this server. As prerequisite to sending mails by the Identity Manager Service is a configured SMTP host.

- NTFRS base server

- Boot server
  There is a boot structure stored on this server. Set this option if the boot structure should be accessedby the Identity Manager Service to make changes to a control file, for example.

- Master SQL server
  The master SQL server is already entereed by initial database migration.

- Home server
  Only servers that are are defined as home server are available when user accounts are added. If a server is classified as a home server, the maximum number of home directories to maintain has to be specified. If this number is less than the given maximum number of directories, the home can be added. Otherwise the addition of a new home directory is refused.

- Profile server
  Servers that are labeled as profile server are available to the user when profile directories are being set up.

- Identity Manager Service installed
  The option <Identity Manager Service installed> cannot be edited in the interface. This option is set internally for the server whose queue is being processed. This option is not automatically removed. If necessary, you can reset this option manually for servers whose queue are no longer enabled using the Job Server Editor.

- Max. number of homes

- Homes created

- Max. home storage space [MB]

- Base path for shares

- Copy process (source server)

- Copy process (target server)

- Coding

9

Managing an Active Directory Environment

- Introduction
- Setting Up Active Directory Synchronization
- Basic Configuration Data
- Active Directory Container Structures
- Active Directory User Accounts
- Active Directory Contacts
- Active Directory Groups
- Reports about Active Directory Groups
- Account Policies for Active Directory Domains
- Setting Up Synchronization with a Microsoft Exchange Environment
- Microsoft Exchange Structure
- Microsoft Exchange Recipients

Introduction

Complex windows environments that contain the Active Directory Service (also refered to as ADS) can be mapped and synchronized in the Identity Manager. Administration of Active Directory objects such as users, contact groups, computers and organizational units is possible in the Identity Manager in hierarchical domain structures.

Company employees are provided with the necessary user accounts in the Identity Manager. For this, you can use different mechanisms to connect employees to their Active Directory user accounts. You can also manage Active Directory user accounts independently of employees and therefore set up administrator user accounts.

Administration of Active Directory groups in the Identity Manager, enables users to be supplied with necessary authorizations. You can set up organizational units in a hierarchical container structure in the Identity Manager. Organizational units (branches or departments) are used to logically organize Active Directory objects such as users, groups and computers. This makes it easier to manage objects.

Setting Up Active Directory Synchronization

Identity Manager Service provides the means to compare data between the Identity Manager database and the Active Directory environment. Prerequistites for synchronization are:

- Installation and configuration of a synchronization server
- Setup of the database for synchronization

The basic synchronization mechanisms are explained in the chapter Data Synchronization in Identity Manager on page 161.

Installation and Configuration of the Active Directory Synchronization Server

In order to set up synchronization with an Active Directory environment, you need a server installed with the following software:

- Windows 2000 Server or Advanced Server with at least Service Pack 2 for Windows 2000, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 or Windows Server 2008 R2
- Microsoft .NET Framework with at least version 3.5, Service pack 1
- Microsoft Software Installation (MSI) service
- Installation of Identity Manager Service from the Setup-CD
  This installation is described in section Installing Identity Manager Tools on page 23 in the Getting Started Manual. Note that you also need to take into account the instructions about installation on a terminal server (see Installing on a Microsoft Windows Terminal Server on page 25).

Next, you configure Identity Manager Service on the synchronization server and start the service. For more information, refer to the section Setting Up a Server for Database Access on page 44 in the Getting Started Manual.

If the server running the synchronization does not have a connection to the Identity Manager database, synchronization is aborted with an error message. Ensure that the server can connect directly to the Identity Manager database!

Identity Manager Service Access Rights Necessary for Synchronization with Active Directory Service

The following access rights are required for the given synchronization root in the Active Directory environment:

- Read
- Write

If the root is the domain object these rights are necessary to make reading and setting domain properties, such as password guidelines for example, possible.

In order to work without restriction under the root object, the access rights

- Create all child objects
- Delete all child objects

are required.

The following access rights are necessary in order to edit specific properties of a user object that cause the access rights list of an Active Directory object to be modified (e.g. ”Cannot change password‟).

- Read permissions
- Modify permissions

Another privilege that is assumed is:

- Modify Owner

Normally, only the administration group has this privilege. When the Identity Manager Service service account is not a member of this group or an equivalent group, it needs to be able to deal with accounts that no longer have permissions set.

The following access rights are required because all object values should be, in principle, editable in the Identity Manager.

- Read All Properties
- Write All Properties

Due to the Active Directory structure, the Identity Manager Service user account should be a subdomain member in the group ”Enterprise Admins‟ in a hierarchical domain structure.

Tips for ”Read Only“ Access Rights

Basically, the part of the synchronization with Active Directory that loads the Active Directory objects into the Identity Manager database, also works when the access rights are read-only and no write access is available.

The following problems can occur:

1. In order to incorporate a user account with read-only access into a group, which may not be the user account’s primary group, Identity Manager Service must have at least write access for the group object.

2. An error condition can occur between the Identity Manager database and Active Directory data when parts of Active Directory that are read-only are added or modified through the Identity Manager administration tools or imported objects. These cases can be excluded with the suitable menu navigation in the administration tools, Identity Manager object access rights and by taking appropriate precautions when importing.

Setting Up the Identity Manager Database for Synchronization with an Active Directory Environment

Effective Configuration Parameters to Synchronize with an Active Directory Environment

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS	The Active Directory area is supported. This is a preprocessor relevant parameter. The database needs to be recompiled after the configuration parameter has been changed.

Prerequisites for reconciliation of an Active Directory environment with the Identity Manager database are that:

- The configuration parameter ”TargetSystem\ADS“ is set. This makes the database components for the Active Directory available for use. The configuration parameter ”TargetSystem\ADS“ is a preprocessor relevant configuration parameter. The database needs to be recompiled after this parameter has been changed. For more infomation read section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and the section Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual.

- The synchronization server is set up. The installation prerequisites are described in the section Installation and Configuration of the Active Directory Synchronization Server on page 202. The server setup in the Identity Manager database is explained in section Declaring the Active Directory Synchronization Server on page 205

- The Active Directory Domains to be synchronized in the Identity Manager are declared. Read more in the section Setting Up an Active Directory Domain on page 206.

- Synchronization is configured and the scheduled tasks are started.
  You decide which Active Directory objects are synchronized between the target system and Identity Manager database and how via the synchronization confiruation. For more information, read section Table Configuring Active Directory Domain Synchronization on page 215

Using the Target System Wizard for Setting Up Synchronization

Tool: Manager

In order to set up the Identity Manager database for synchronization with an Active Directory environment, an wizard is available in the category <My Identity Manager>\<Target system wizards>\<Configure Active Directory Service>. This wizard covers the most important configuration stages for an initial synchronization implementation. The assitant takes you through the basic configuration stages from setting up the Active Directory domain in the Identity Manager database to the initial synchronization with an Active Directory environment. The initial synchronization does not cover all the Active Directory objects but simply the objects that are required for the program to run. Basically, the wizard does not apply any settings to the Active Directory administrated by the Identity Manager. All settings are modifications to the behavior of the Identity Manager. They are saved in the Identity Manager database.

The following work stages are executed by the assitant:

- Setting up an Active Directory domain with the database
- Setting up the synchronization server in the database
- Starting the initial synchronization

Other configuration steps may be necessary for the administration of the Active Directory environment by the Identity Manager.

Declaring the Active Directory Synchronization Server

Tool: Manager; Identity Manager with the application role <Target system>\<Active Directory>

All Identity Manager Service actions are executed from the synchronization server. The entries which are necessary for synchronization and administration with the Identity Manager database are processed by the synchronization server.

Configure new synchronization servers in the category <Active Directory>\<Server>. A minimum of the following data has to entered for a synchronization server:

- Server
  Server name
  The server name is used to compose the queue name for the corresponding Job server. The process steps are requested in the Job queue with exactly these queue names.
- Hardware
  Name of the hardware that the synchronization server is installed on.
- Language
  Language setting for the synchronization server

- Identification as domain controller

Setup the server hardware initially without a target system account (option <AD account>) and without an Active Directory container because there are no Active Directory containers declared in the Identity Manager database when the synchronization server is initial configured. Active Directory containers are determined during synchronization and can be assigned to the server hardware afterwards.

The meaning of the other input fields and options is described in section Synchronization Server Administration on page 196. This input, however, is not relevant for the function of the server as synchronization server.

Once the synchronization server has been declared in the database a corresponding entry is made for a Job server that is made available by Identity Manager Service for processing target system specific processes. This queue needs to be entered in the Identity Manager Service configuration file. See section Job Server Declaration on page 207 in the Resource Kit Manual

Setting Up an Active Directory Domain

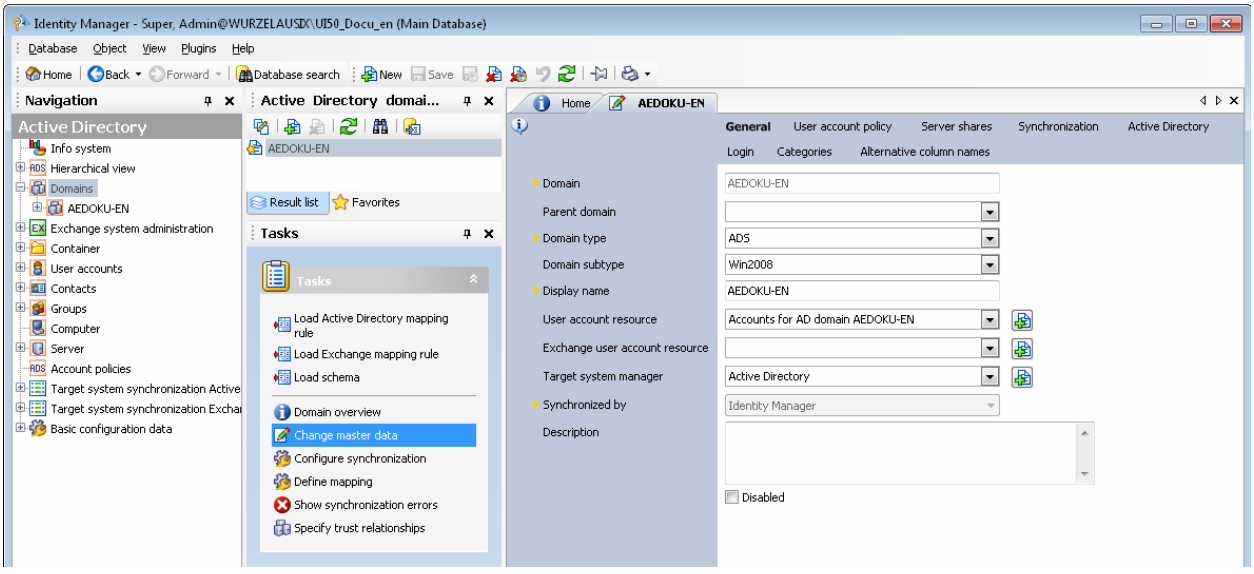
Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

In the Manager, map Active Directory domains for synchronization to the category <Active Directory Service>\<Domains>. To do this, log on with a role based authentication module from the application role <Target systems>\<Active Directory Service>. Enter the data required for an Active Directory domain on the form <Change master data>.

General Master Data for an Active Directory Domain

You can display the Active Directory domain to be synchronized with the Identity Manager database, in the category <Active Directory Service>\<Domains>.

Setting up an Active Directory Domain



You need to enter the following information for the Active Directory Domain:

- Active Directory Domain name
  Enter the Active Directory domain NetBIOS name. This corresponds to the pre-Windows 2000 domain names. The domain name cannot be changed in retrospect.

- Parent Domäne
  Enter a parent Active Directory domain in order to map a hierarchical domain structure. The full name and the defined name (tab <ADS>) are automatically updated via templates.

- Domain type to identify the domain
  Select the domain type ”ADS“ for an Active Directory domain.

- Domain subtype
  The domain subtype represents the Active Directory function level. There are several features available in Active Directory at function level. Refer to the documentation for the appropriate Windows server to find out which function levels are supported by the domain controller operating system to be implemented. The following function levels are supported in Identity Manager:
  - Windows 2000 (Win2000)
  - Windows Server 2003 native (Win2003 native)
  - Windows Server 2003 mixed (Win2003 mixed)
  - Windows Server 2008 (Win2008)
  - Windows Server 2008 R2 (Win2008 R2)

- Active Directory domain display name
  The display name is used to display the Active Directory domain in the user interface. This is preset with the Active Directory domain NetBIOS name. However, the display name can be changed.

- User account resource
  This input is required if the Active Directory user account manages this Active Directory domain via a user account resource. For more information, see section Managing Active Directory User Accounts with User Account Resources on page 234.

- Exchange user account resource
  This input is required if the mailboxes for this Active Directory domain are managed via a user account resource. For more information see section Administration of Microsoft Exchange Mailboxes via User Account Resources on page 284.

- Target system manager
  Select the Identity Manager application role whose members are responsible for the domain administration. User the button next to the input field to create a new application role. Target system managers only edit the object from Active Directory domains that are assigned to them. Therefore, each Active Directory domain can have a different target system managers assigned to them. In the Manager, the application roles are displayed in the category <Basic configuration data>\<Target system managers> abgebildet.

- Synchronized by
  Specify how the data will be synchronized between the Active Directory domain and the Identity Manager. Choose between ”Identity Manager“, ”FIM“ and ”No synchronization“.

  Identity Manager: data synchronization between the Identity Manager database and the Active Directory domain is executed by the synchronization components from the Identity Manager.
  FIM: data synchronization between the Identity Manager database and the Active Directory domain is executed by the Microsoft Forefront Identity Manager.
  No synchronization: no changes are automatically transfered from the Identity Manager database to the Active Directory domain.

  You can only specify the type of synchronization when a new client is added. Once it has

been saved, no changes can be made. If you select ”No synchronization“ you can define custom processes to exchange data between the Identity Manager and the Active Directory domain.

- Enable recycling bin/retention time
  As from ”Windows Server 2008 R2“ function level you can input additional data for the Active Directory recycling bin“. The properties <Enable recycling bin> and <retention time> are loaded via synchronization and cannot be changed in Identity Manager.

- Use recycling bin
  Here it is specified whether the Active Directory recycling bin should be used by Identity Manager processes. Refer to section Deleting and Restoring Active Directory User Accounts on page 239 for more information.

- Description
  Additional information about Active Directory domains.

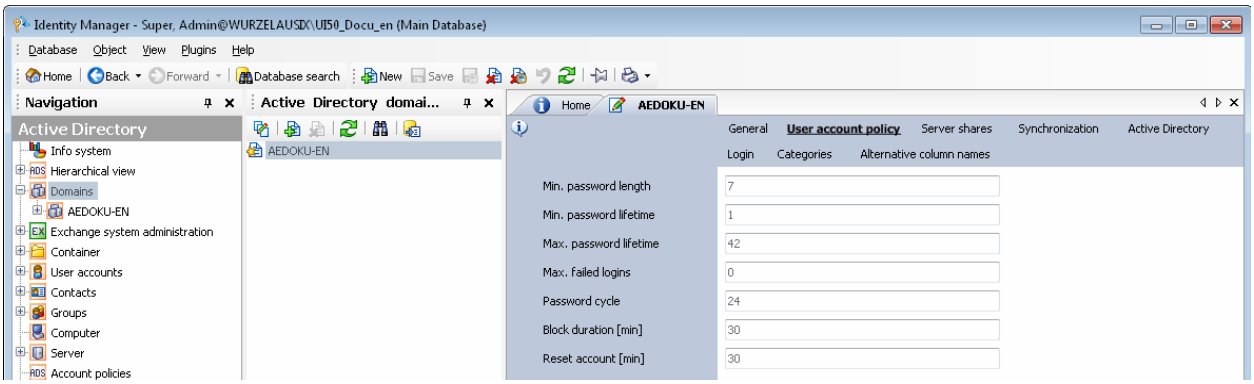
- Specifies whether this is a master domain

- Specifies whether the domain is enable or temporarily disabled
  This option is interpreted in various processes for initial filling of an Active Directory domain.

Specifying User Account Policy

On the <Account policy>, you can specify the requirements for password allocation in an Active Directory domain. This information is passed on to the domain as the default settings and are valid for all new Active Directory user accounts.

User Account Policy for specifying an Active Directory domain



A user account policy includes:

- Minimal length of the password
  Enter the minimum number of characters the password has to have.

- The minimum lifetime time of a password
  Enter the length of time a password has to be used before the user is allowed to change it.

- The maximum lifetime of a password
  Enter the length of time a password can be used before a new password has to be set.

- The maximum number of incorrect password attempts
  Set the number of invalid passwords. If the user has reached this number the account is blocked.

- Password cycle
  Enter the number of new passwords that a user has to user before an ‘old’ one can be reused.

- The length of time the account is blocked in minutes
  Enter the length of time that the account is disabled before it is automatically reset.

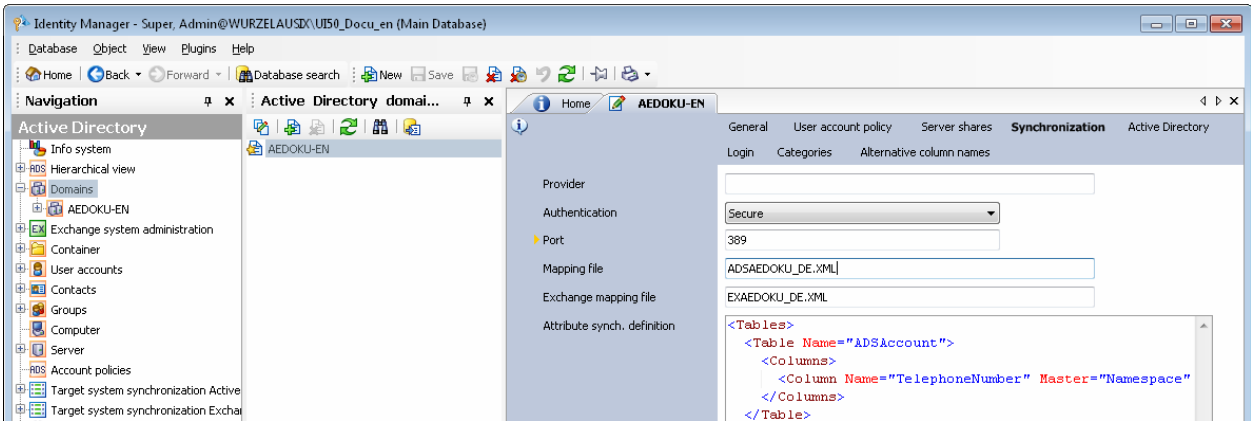
- The length of time in minutes before the account is reset
  Enter the length of time that the user account should be blocked between two incorrect password entries.

You can setup more than one user account policies for Active Directory domains with the ”Windows Server 2008 R2“ function level. For more information, see section Account Policies for Active Directory Domains on page 255.

Customizing Sychronization Data

On the <Synchronization> tab you customize the data for data synchronization between the Identity Manager database and the target system environment. You can make these modifications for each Active Directory domain because the requirement vary from domain to domain.

Customizing Data Synchronization



- Provider selection
  If there are several providers available for accessing the target system, you should enter the provider to be used here. This functionality is currently not implemented for Active Directory.

- Authentification data
  Here you can specify the authentication type for logging into the target system as an addition to the user account and password. There is a choice of several authentication types, for example, ”Encryption (SSL)“, ”Secure“. You can find a short explanation of each method on ”http://msdn.microsoft.com/de-de/library/system.directoryservices.authenticationtypes.aspx“.

- Port
  As addition to the user account and password, you can enter the number of the communications port on the target system server.

- Mapping file
  The mapping file contains the templates for mapping target system specific objects, such as users, groups or hardware objects, between the Identity Manager database and Windows NT domains. The evaluation is executed using target system specific process components. An external mapping file only has to be given if the default mapping for the data should not be

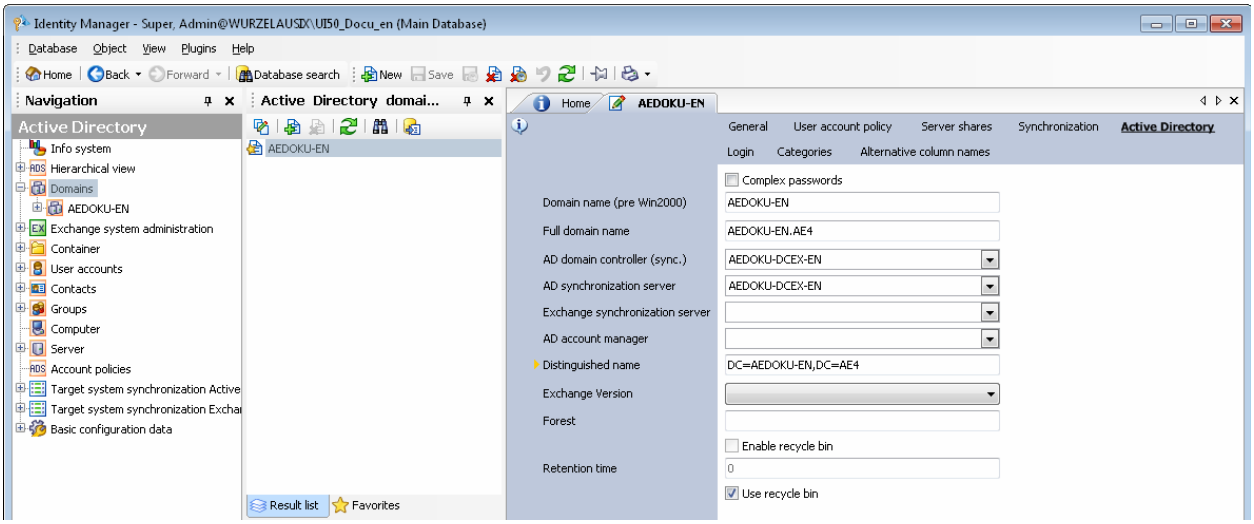
used. This external mapping file must exist on the synchronization server. If no path is given, the mapping file has to be in the Identity Manager Service install directory on the synchronization server. Refer to the chapter Customizing Mapping rules on page 180 for more information.

- Attribute sync. definition
  You can specify the master for data synchronization for individual target specific object properties with the attribute alignment definition. Specify the master data via the form <Define mapping>. This displays the definition as an XML structure. You can also find information in section Specifying the Data Master for Object Properties on page 192 for more information.

Active Directory Specific Master Data

The <ADS> tab is visible when a domain is marked with the domain type ”ADS“.

Target System Specific Input for Active Directory Domains



The following input is required:

- Input to specify whether complex passwords are used or not

- Domain (preWin2000)
  Enter the pre-Windows 2000 domain name. This domain name is used to log an Active Directory Domain onto a workstation that is running Windows NT 3.5x / 4.0.

- Full domain name
  Enter the domain names for the Active Directory domain in DNS-Syntax:

  ```
  Name of this Domain.Name of parent domain.Name of domain origin
  ```

  Example:

  ```
  DHW2k01.Testlab.questsoftware.com
  ```

- Active Directory synchronization server
  Select the server to be used for reconciliation between the database and the Active Directory environment. This server has to be a domain controller and has to be entered into the Identity Manager database. You can read more in the section Declaring the Active Directory Synchronization Server on page 205.

  Take note of the following:

Only those servers are displayed in the Identity Manager that have an Active Directory container in the Active Directory domain that they manage. Therefore, it may be necessary in certain circumstances to enter the synchronization server via the Manager.

- Exchange synchronisation server
  This input only relevant for synchronizing with a Microsoft Exchange system. For more infomration see section Active Directory Domain Extended Master Data for Synchronizing with Microsoft Exchange on page 263.

- Active Directory account manager
  The manager for the Active Directory domain.

- Distinguished name
  The distinguished name is determined via a template fromthe full domain name and should not be edited.

- Exchange version
  This information is only relevant for sychronizing with a Microsoft Exchange system. See section Active Directory Domain Extended Master Data for Synchronizing with Microsoft Exchange on page 263 for more information.

- Forest
  The name of the forest that the domains belong to. This name should be given if group memberships are mapped cross-domain. See section Validity of Group Memberships on page 247.

Login Data

Enter the user account and password to log into a Active Directory domain on the <Login> tab. Give the user account as a defined LDAP name.

Example:

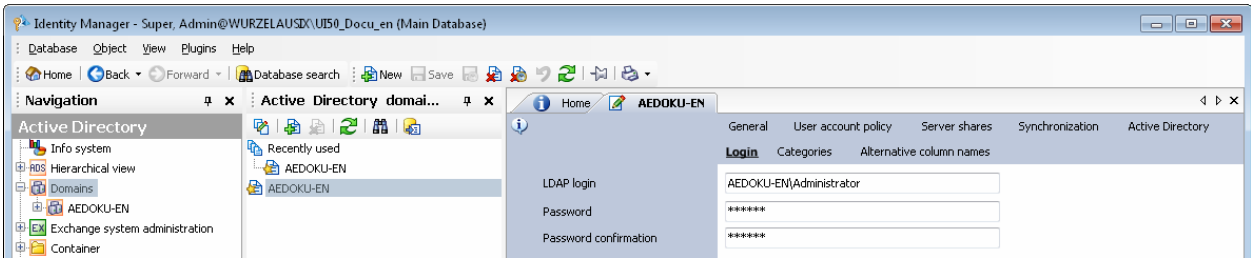
The syntax of the defined LDAP name for the user account ”Administrator“ in container ”users“ in the domain ”DHW2k01.Testlab.QuestSoftware.com“ is:

```
CN=Administrator,CN=Users,DC=DHW2k01,DC=Testlab,DC=questsoftware,DC=com
```

Use a user account with administrative rights in the Active Directory environment. This account is used to synchronize properties of Active Directory objects.

If the LDAP account does not exist, the Active Directory object properties that are not set are passed to the Active Directory environment with a space character. This can lead to problems on the screen.

Active Directory Domain Login



Configuration of Extended Properties for an Active Directory Domain

Active Directory groups can be selectively inherited by Active Directory user accounts in Identity Manager. To do this, users and group are divided into categories. The categories can be selected freely and are specified via a defined template. The functionality of inheritance is described in more detail in the section Inheriting Group Memberships Based on Categories on page 82.

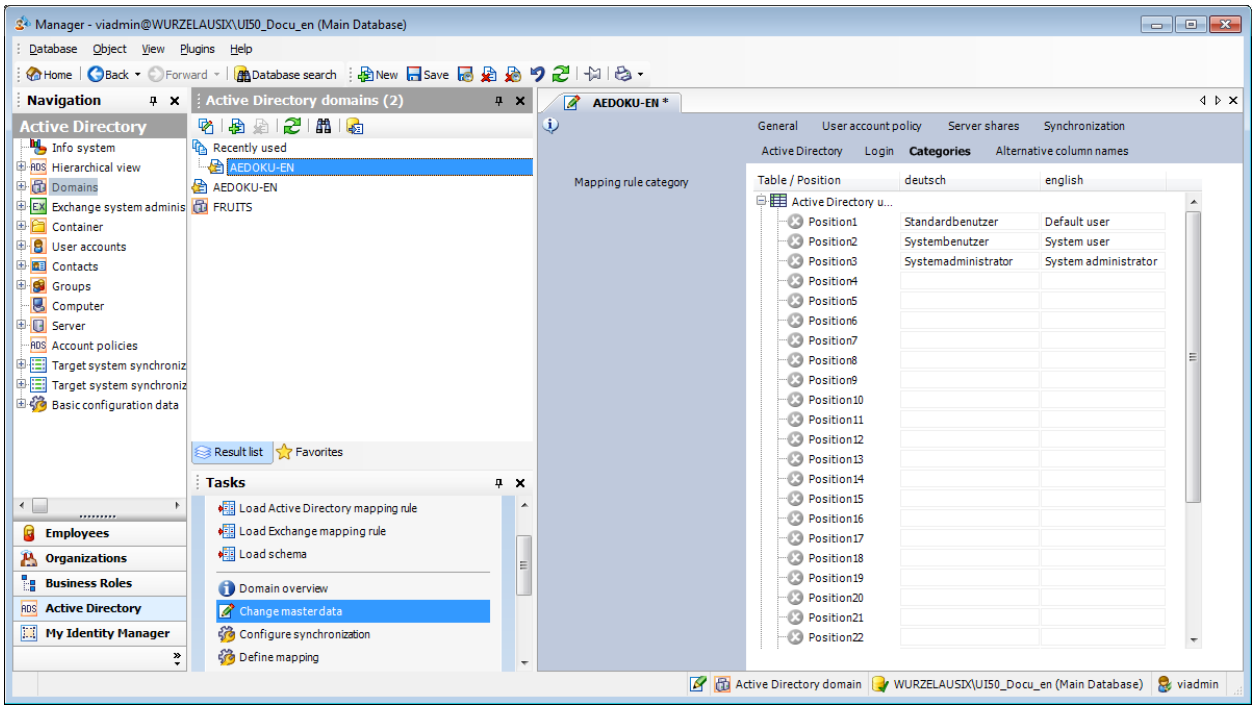
The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent users. In the group table, you enter the categories for the target dependent groups. Each table contains the category items ”Position1“ to ”Position31“. To use the categories, enable them by clicking on the icon next to the item description. Enter the descriptions in the appropriate language for displaying the categories in the user interface.

To use categories, define them as follows:

- Open each member tree in the user account table or the group table.
- Enable the category by double clicking on the icon next to the item description.
- Enter a name for the Active Directory user accounts or group category for Identity Manager in the column for the respective login language.

Further customizing is relevant for displaying object columns in an Active Directory domain on the user interface forms. If you require different names for the input fields to the ones on the master data form, you can specify a alternative column name for each object type here.

Configuration of Extended Properties for an Active Directory Domain

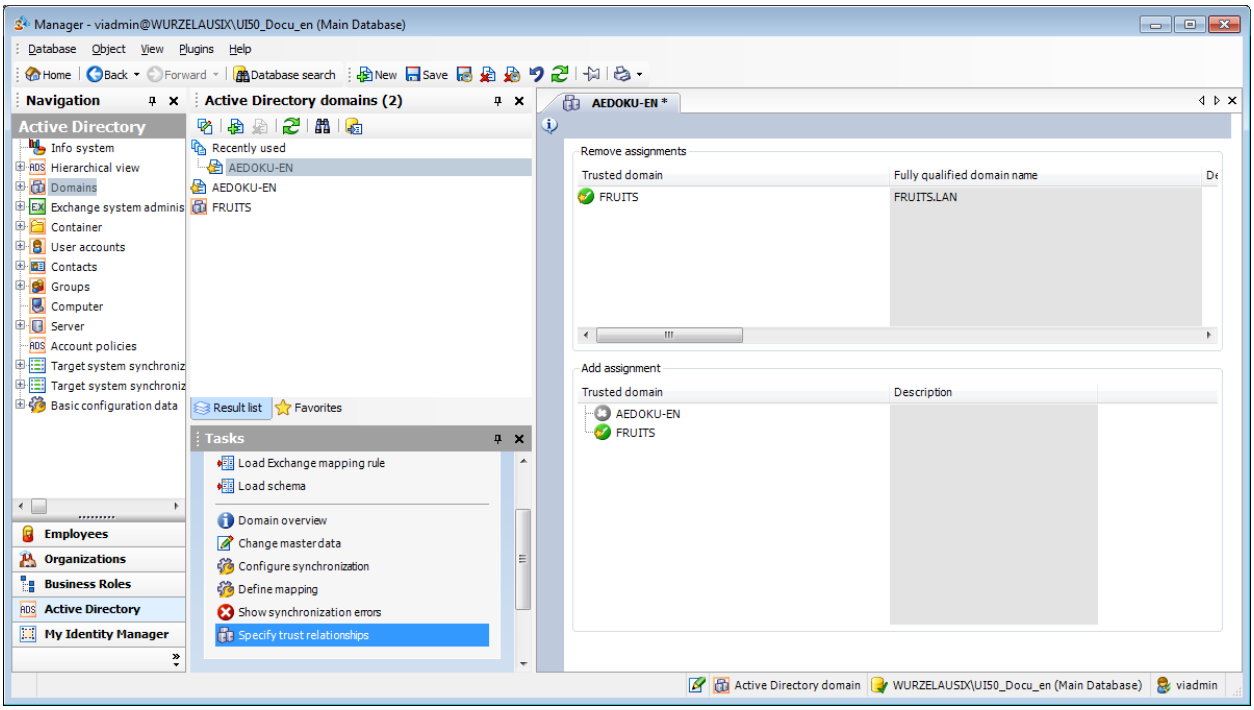


Trusted Domains

Read the documentation for the your Windows server for an explanation of the concept of trusted domains under Active Directory.

Users and resources can access other domains depending on the trust of the domains.

Setting Up Trusts



Reports about Active Directory Domains

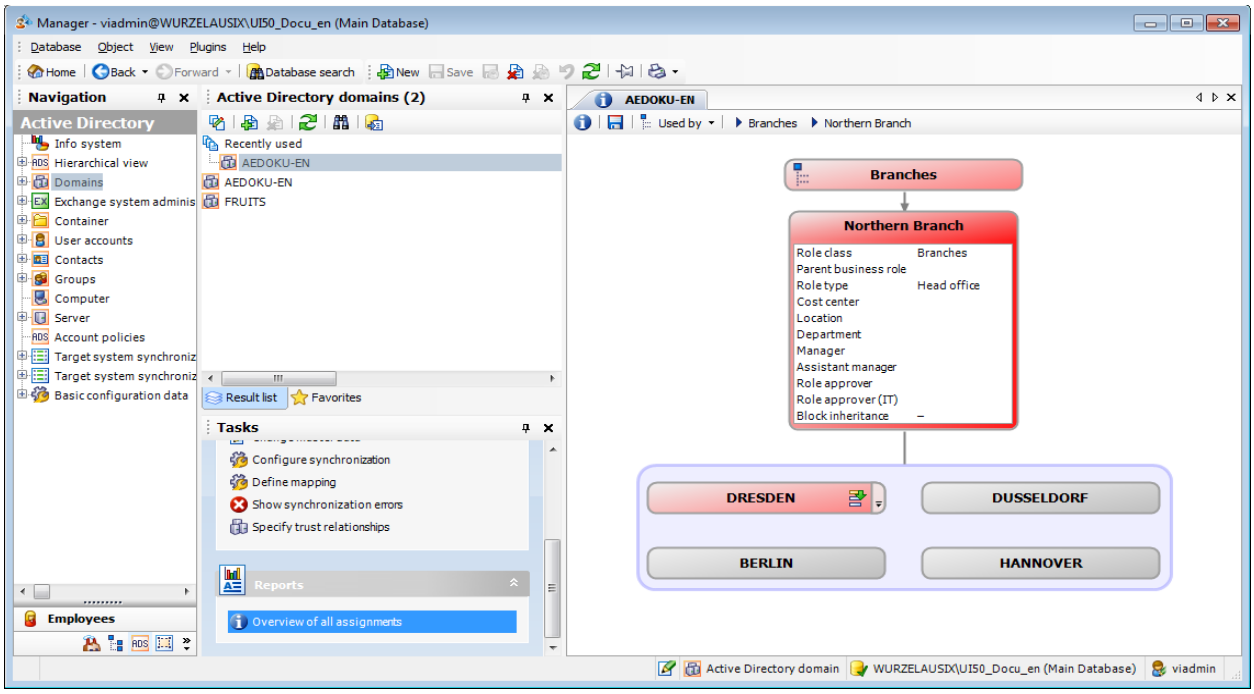
Identity Manager provides several reports that prepares information about the selected base object and its relations to other objects in the Identity Manager database. The following reports are available for Active Directory domains.

Overview of all Assignments

This report shows all employees that are assigned at least one Active Directory user account in the selected Active Directory domain. In this case, directly assigned objects are taken into account as well as

objects obtained via inheritance. The report shows which roles of a role class the employee belongs to. What you get is an organigram of the different role classes for the selected Active Directory Domain.

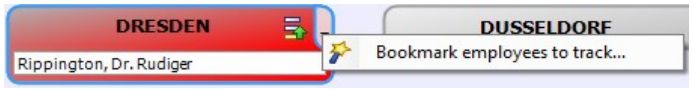
Report "Overview of all Assignments" for an Active Directory Domain



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that violate the role and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

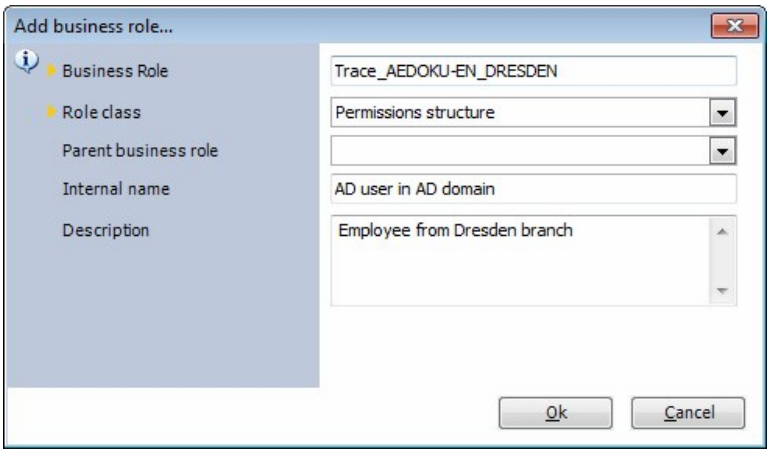
Bookmark Employee for Tracking



To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Configuring Active Directory Domain Synchronization

Tool: Manager

Take the basic information about data synchronization from the section Data Synchronization in Identity Manager on page 161. The following steps are required to synchronize between an Identity Manager database with an Active Directory:

- Customize configuration parameters that are relevant for synchronization.
  For more information read section Configuration Parameters for Synchronization with an Active Directory Environment on page 216.

- Configure synchronization.
  The basic procedure is described in section Data Synchronization in Identity Manager on page 161. Special feature of synchronization with an Active Directory domain are given in section Special features of Active Directory Domain Synchronization Configuration on page 217.

- Define a mapping
  The basic procedure is described in section How to Define a Mapping on page 175.

Extensive information about synchronization analysis and processing synchronization error is found in section Synchronization Analysis on page 176.

Configuration Parameters for Synchronization with an Active Directory Environment

The following table only lists configuration parameters that are relevant for scheduled synchronization. There may also be other configuration parameters be applied for target system relevant actions, for example, inserting, changing or deleting a user account in the database and the subsequent transfer into the target system via Identity Manager Service.

The complete list of configuration parameter is found in the Designer. Edit configuration parameters in the Designer. For more information, read chapter System Configuration Parameters on page 214 in the Configuration Manual.

Certain configuration parameters are preprocessor relevant. You have to compile the database if you make any changes to these parameters. Read section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and section Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual for more information.

Configuration Parameters for Synchronizing an Environment

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\Default-Address	This configuration parameter contains the default email address for messages when actions in the target system fail.
TargetSystem\ADS\EnableRAS	Preprocessor relevant configuration parameter for controll the database components for Remote Access Sevice (RAS) properties of the target system Active Directory. If the parameter is set, Active Directory RAS properties are supported. If the parameter is not set, RAS properties are not taken into account. This reduces the time required for synchronizing Active Directory objects and the for changes to individual objects. Changes to the parameters require recompiling the database.
TargetSystem\ADS\IsOperational	This configuration parameter specifies whether the target system access is tested before the action takes place. If the parameter is set, the system is tested for availability before the action takes place.
TargetSystem\ADS\MaxFullsync-Duration	Gives the maximum runtime for synchronization. No recalculation of group memberships by the DBScheduler can take place during this time.
TargetSystem\ADS\MaxSyncDelayTime	Maximum time minutes before changes in the target system are synchronized across the domain.
TargetSystem\ADS\Person-AutoFullsync	Automatic employee assignment for Active Directory user accounts creating via synchronization is executed depending on the mode given here. For more information see section Automatic Assignment of Employees to User Accounts on page 40.

Configuration Parameters for Synchronizing an Environment

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\RedoDelay	This configuration parameter specifies the delay time after which an incompleted modification on a target system object is repeated. The input is in minutes.
TargetSystem\ADS\ReplicateImmediately	This configuration parameter is used to speed up synchronization of modifications between two domain controllers. When set, the accumulated ADmodifications are immediately replicated between domain controllers.
TargetSystem\ADS\SingleThread	Specifies whether synchronization objects should be saved synchronously. The objects are saved asychronously by default. If the parameter is set, saving is synchronous, which increases the synchonization runtime!
TargetSystem\ADS\TerminalProperties	Preprocessor relevant configuration parameter for controlling the database components of the target system Active Directory. If the parameter is set, the terminal properties are available. When the configuration parameter is active, the terminal properties of the Active Directory objects are snychronized. If the configuration parameter is not set, the terminal properties are not taken into account. This reduces the time required for synchronizing and also for making changes to ADS objects. Changes to the parameter require recompiling the database.

Special features of Active Directory Domain Synchronization Configuration

Read section Data Synchronization in Identity Manager on page 161 for details about the basic synchronization configuration. At this point, we are only going to look at the special features relevant to the synchronization configuration for Active Directory domains. The following configuration tasks are available for synchronizating an Active Directory domain.

Configuring Synchronization

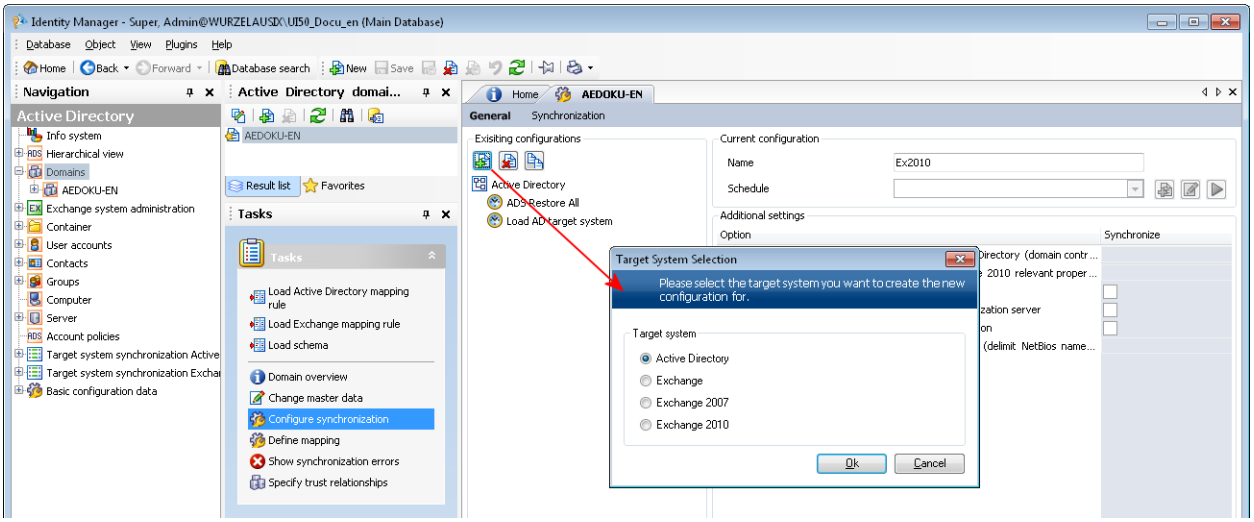
Use this form to set up the synchronization configuration. Enter the basic synchronization configuration and the schedule on the <General> tab. If necessary, you can manually start synchronization from here. On the <Synchronization> tab, specify how objects should be handled during synchronization.

For a new synchronization configuration, select the target system ”Active Directory“. The following are available:

- ”Active Directory“ for synchronzing and Active Directory
- ”Exchange“ for synchronizing with a Microsoft Exchange Server 2000, Microsoft Exchange Server2003 or Microsoft Exchange Server 2007
- ”Exchange 2010“ for synchronizing with a Microsoft Exchange Server 2010

The configuration can then be executed as described in section How to Configure Synchronization on page 163.

Selecting the Target System in the Synchronization Configuration



The following options are available on the <Additional settings> pane on the <General> tab:

- Synchronize Active Directory system containers
  When this option is set, containers that are labeled as system containers are synchronized betweem target system and the Identity Manager database.

- Synchronize Active Directory system containers with advanced functions
  When this option is set, system containers with ”advanced features“ (ShowInAdvancedView-Only) are synchronized between target system and the Identity Manager database.

- Exclude Remote Access Service (RAS) propertes from synchronization
  Use this option to specify whether RAS properties should be included.

  Please note:
  RAS properties can only be loaded if the configuration parameter ”TargetSystem\ADS\Enab-leRAS“ is set.

- Exclude Terminal Service properties from synchronization
  Use this option to specify whether Terminal Service properties should be included.

  Please note:
  Terminal Service properties can only be loaded if the configuration parameter ”TargetSys-tem\ADS\TerminalProperties“ is set.

- Also look for group members in following domains (delimit NetBios names with a comma)
  Group membership of Active Directory user accounts in these domain is determined during synchronization. These may be domains in a domain hierarchy or trusted domains.

Defining a Mapping

Use this task to specify how the structure of properties belonging to the object types to be synchronized is mapped in the database and in the target system. The configuration of assignments is described in detail in section How to Define a Mapping on page 175.

Displaying Synchronization Errors

This task provides an alternative method for analysing the synchronization in addition to the Identity Manager Service log file. The objects and dependencies which failed during synchronization are shown on the form. A detailed description of the error is displayed. The section Logging Synchronization Errors on page 176 provides more detailed information.

Speeding Up Synchronization by Including an Update Sequence Number

The Update Sequence Number (USN) is a sequencial number that is incremented when changes are made to Active Directory objects. It is local to the server, an Active Directory object hast its own USN on on every Active Directory domain controller. In the Identity Manager data model, Active Directory objects (Active Directory containers, Active Directory user accounts, Active Directory groups and hardware) are equiped with USN.

You can use USN comparison to avoid unnecessarily updating objects that have not changed since the last synchronization when Active Directory objects are synchronized with the Identity Manager database. If Active Directory object synchronization is run on the same server and the configuration parameter is set, change operations are inhibited for the Identity Manager and Active Directory objects that have the same USN. See section How to Speed up Synchronization on page 174 for more information.

Please note that when you synchronize taking USN in account, not only are group memberships (object type ”ADSGroupMember“) but also the groups (object type Group“) are synchronized. The USN for an Active Directory group increases each time a change is made to the object in the target system. Even adding and deleting group memberships results in a change to the group object‘s USN. During synchronization all target system group objects are monitored and the current USNs are copied to the database if they have changed. It is only possible to run a correct comparison of group memberships with the help of updated USNs.

Basic Configuration Data

Target System Manager

You can assign employees in the Identity Manager to every Active Directory domain that can edit the objects in this domain in the Identity Manager. To do this, assign an application role <Target system manager> in the Active Directory domain general master data. Assign the employees to this role that are authorized to edit Active Directory domains in the Identity Manager.

Edit target system managers for Active Directory in the Manager in the category <Active Directory>\<Basic configuration data>\<Target system managers>\<Active Directory> or in the Identity Manager in the category <Identity Manager Administration>\<Target systems>\<Active Directory>. You can find more detailed information about application roles in section The Identity Manager Roles Model on page 61.

Active Directory Container Structures

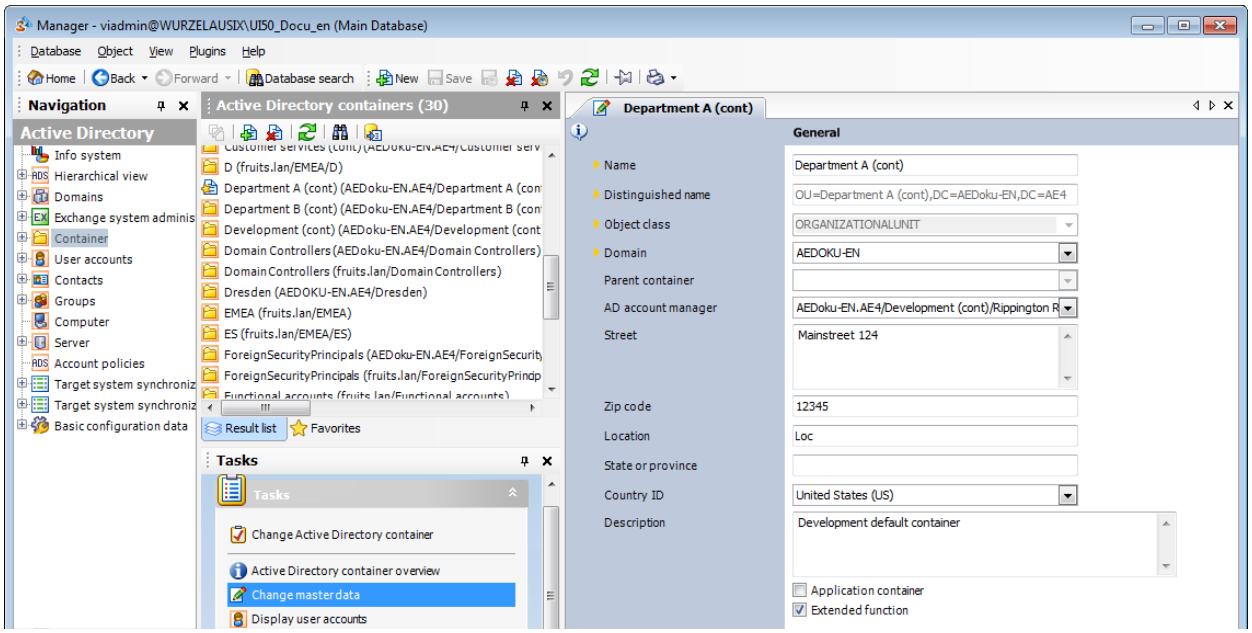
Active Directory containers are displayed in a hierarchical tree structure. The containers that already exist can be loaded from Active Directory environment into the Identity Manager database by synchronization. System containers, which are entered into the Identity Manager database are labeled correspondingly. These are only taken into account in the synchronization when the relevant configuration option is set.

Setting Up Active Directory Containers

Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

Active Directory containers are displayed in the category <Active Directory Service>\<Container>. Enter the data required for an Active Directory container on the <Change Master Data> form. Ensure that you fill out all the fields marked as mandatory.

Setting up an Active Directory Container



Enter the following data for an Active Directory container:

- Container name
  This name cannot be changed retrospectively.

- Distinguished Name
  The distinguished name for the new container is made up from the container name, the object class, the parent container and the domain and cannot be modified.

- Object class
  The object classes that are displayed are read in from the database during synchronization with the Active Directory environment. You can, however, enter additional object classes in the input field. Other properties can be edited depending on the object class. You should set up newly added Active Directory containers as organizational units (object class ”organizational unit“). Organizational units (e.g. branches or departments) are used organize Active Directory objects, such as users, groups and computers, in a logical way and therefore make administration of the objects easier. organizational units can be managed in a hierarchical container structure.

- Container domain

- Parent container
  If you want to implement a hierarchical container structure, specify the parent Active Directory container. The distinguished name is automatically updated via templates.

- AD account manager
  Manager for the Active Directory container.

- Address data
  Address data includes street, zip code, location, state and country code.

- Description
  Additional information about the Active Directory container.

- Application container
  Mark the Active Directory container for software distribution with the option <Application container>. Refer to the section about software distribution in Active Directory in the Configuration Manual Managing Application Groups in Active Directory on page 286.

- Extended function
  Containers that are marked with the option <Extended function> are only shown in the Active Directory user account and computer Manager when an advanced mode console view is active. This option is used as a filter criterium for other representations of the container in the Identity Manager Manager.

Addtional Tasks for Managing Active Directory Containers

Once you have enter the master data you can apply several other tasks to the Active Directory container, You see the most import information about an Active Directory container on the overview form. The task view contains different forms with which you can run the following tasks.

Moving Active Directory Containers

To change (move) an Active Directory container, run the task <Change Active Directory container>. Active Directory containers can only be moved within an Active Directory domain.

Check assignment of Active Directory User Accounts, Active Directory Groups and Active Directory Computers

You can check the assignment of users, groups and computers in the container structure via the assignment forms <Show user accounts>, <Show groups> and <Show computers>. Add new users, groups and computers to the selected Active Directory container using the additional task displayed when you change forms. The Active Directory container data already set in the respective Active Directory objects via the these tasks.

A mechanism to monitor membership has been implemented because Active Directory only supports a limited number of members in containers. Refer to the Configuration Manual, section Monitoring the Number of Memberships in Active Directory Groups and Active Directory Containers on page 293 for more information.

Active Directory User Accounts

Configuration Parameters for Setting Up User Accounts

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\PersonAutoDefault	This mode enables automatic assignment of employees to user accounts created in the database.
TargetSystem\ADS\PersonAutoFullsync	This mode enable automatic assignment of employees to user accounts created in the database via synchronization.

The Identity Manager manages Active Directory user accounts in an Active Directory environment. In Active Directory, a user is a security principal, that means an Active Directory user account can log onto

an Active Directory domain. A user receives access to network resources through group membership and access permission.

The Identity Manager works with different methods to create user accounts and to assign employees to user accounts.

- Employee and Active Directory user accounts can be manually entered and assigned to each other.
- Employees can automatically obtain their Active Directory user accounts using user account resources. If an employee does not have a user in an Active Directory domain, a new Active Directory user account is created. This is done by assigning user account resources to an employee using the integrated inheritance mechanism followed by process handling. This method is described in more detail in the section Managing Active Directory User Accounts with User Account Resources on page 234.
- When an Active Directory user account is added, an existing employee is automatically added or a new one is created if necessary. In the process, the employee master data is created based for existing user master data. This mechanism can follow the creation of a new user account by manual addition or by synchronization. This method, however, is not the Identity Manager default method. This method is explained in section Managing Active Directory User Accounts with User Account Resources on page 234.

The basic mechanisms are dealt with in the chapter Employees and User Accounts on page 25

Entering Active Directory User Account Master Data

Tools: Identity Manager with application role <Target system>\<Active Directory>; Manager

An Active Directory user account can be connected to an employee in the Identity Manager. Depending on the user's manage level, certain properties of the employee can be passed on to the user account. In the same way, Active Directory user accounts can be managed separately from employees, for example, when dealing with administration users.

Active Directory user accounts are displayed in the category <Active Directory Service>\<User accounts>. You can manually enter the required data on the form <Change master data> and rework it if necessary. Note that all compulsory marked fields are entered.

It is recommend that user account resources are used to set up an Active Directory user account for a company employee. If you do use an Active Directory user account resource to set up the user, some of the master data that is described in the following is created using templates, e.g. Active Directory containers, Home and profile servers. Certain employee master data is inherited using employee Active Directory user templates. The amount of data, in this case, is based on the default manage level for the user accounts resource. The templates supplied should be customized as required.

General Master Data for an Active Directory User Account

Add general data for an Active Directory user account on the <General> tab. You assign an employee to a user account from the <Employee> pop-up menu. If the user account was created using a user account resource, an employee will already be entered. If you use automatic employee assignment, a associated employee is created and entered into the user account when the user account is saved. If you do not use any of these methods but manually create the user account, you can also assign an employee manually to the user account.

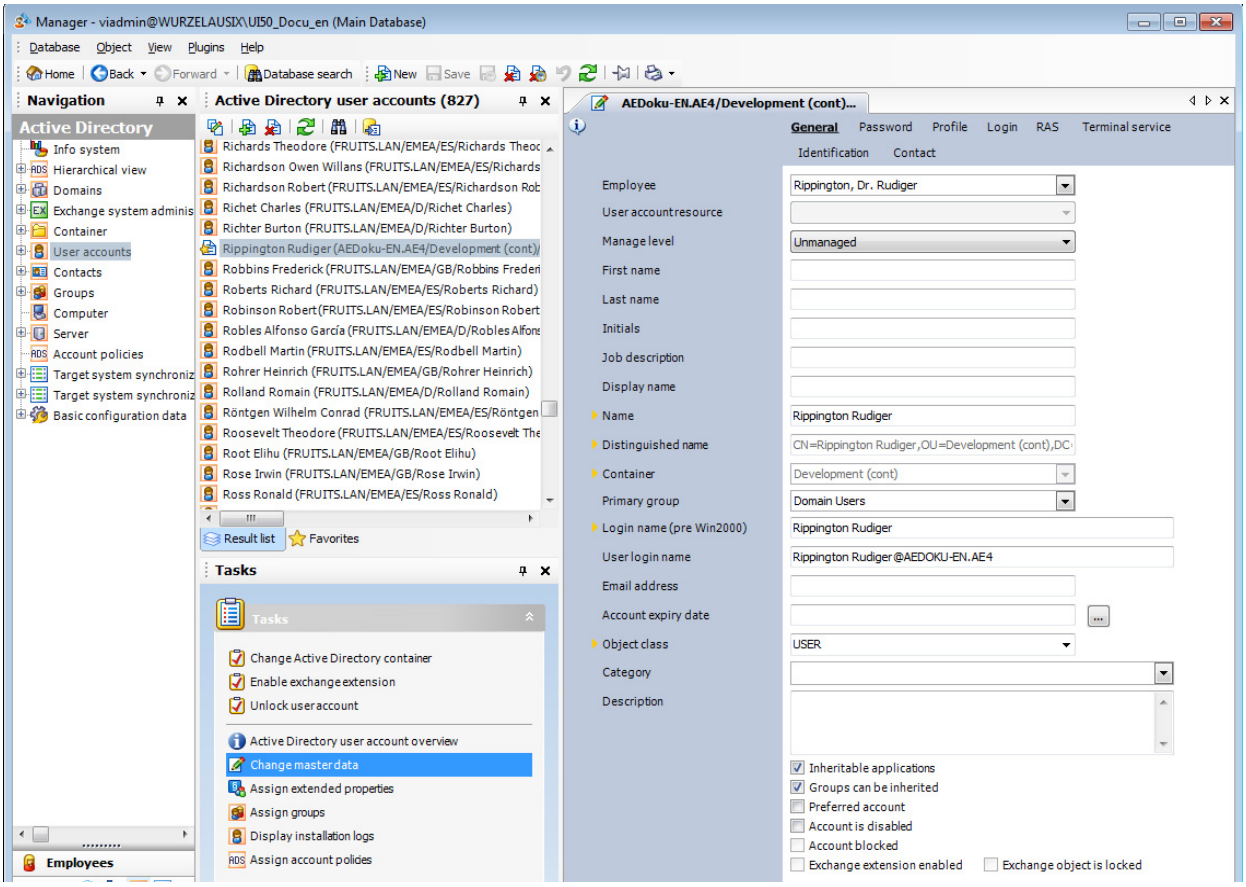
When user account resources are assigned to an employee or a resource to a company structure, an associated ADS user account is created in the Identity Manager with the integrated inheritance mechanism and the process handling that follows. If the process handling fails because, for example, not all the neccesary IT operating data could be found, you can also create the ADS user account manually

and, at the same time, select the user account resource to use. Only the user account resources that are already assigned to the employee are shown in the pop-up menu.

The user account manage level is decided by the range of the employee's properties that are passed on to the user account. The Identity Manager's default installation is configured for the manage levels "Unmanaged" and "Full managed". User accounts with the manage level "Unmanaged" are merely linked to an employee but do not inherit other properties. User account with the manage level "Full managed" inherit defined employee properties. You can define other manage levels depending on the company's requirements.

When a user account is created using a user account resource, the default manage level of the user account resource is used and is transfered to the user account. Normally, the manage level "Full managed" is used as default. If you create the user account manually or with automatic employee assignment, the manage level is "Unmanaged". You can change the levels after the user account has been saved with the pop-up menu <Manage level>, provided that the Active Directory domain has a user account resource.

General Master Data



Enter the general data required for an Active Directory user account such as name, surname and initials. The display name and the user account name are formatted using this data.

Select the Active Directory container that user should be used created in. The Active Directory container is determined from the company IT data for the assigned employee depending on the manage level of the user account. The name defined for the user account is detemined when the Active Directory container is selected.

You can specify a primary group for the user. Synchronization with the Active Directory environment assigns the user to the group ”Domain users“ by default. This membership modification is applicable for users that log on over a Macintosh service. Only Active Directory groups that are assigned to the user are available as primary groups.

You need to enter the login name for the previous version of Active Directory as well as a user login name for the user. The login name (pre Win2000) is formatted from the employee’s central user account depending on the manage level of the Active Directory user account. If you have already established the Active Directory container and entered the login name (pre Win2000), the user login name is created following the formatting rule as shown:

```
Logon name (pre Win2000) @ADS Domain name, the domain where the user account is
found
```

This formatted user logon name corresponds to the user’s principle name in Active Directory.

You can enter more email addresses for an Active Directory user account. Email addesses formatted from the employee’s default email address depending on the manage level of the user account.

Specifying an expiry data for the account has the effect that the logon for this user account is blocked as soon as the given date is exceeded. If you specify a date for the last day of work, depending on the user account manage level, it is automatically taken as the expiry date. If an account expiry date is already entered, it is overwritten. If you delete the date for an employee last day of work, the expiry date remains intact!

By default, you set up Active Directory user accounts in the Identity Manager with the object class ”User“. However, the object class ”InetOrgPerson“ is also supported that is used by other LDAP and X500 directory services to display user accounts. You can also enter additional object classes directly into the input field.

User categories are relevant for inheriting Active Directory groups. Active Directory user accounts can selectively inherit Active Directory groups. To do this the user and groups are divided up. Use the pop-up menu <Category> to allocate one or more categories to the Active Directory user account. For more information read the section Inheriting Group Memberships Based on Categories on page 82.

You can assign applications and application packages to an employee. If this employee has an Active Directory user account then this account becomes a member an application’s application group. Prerequisite for taking on this account in the application group is to set the option <Application inheritable> for this user account and the existance of the application group in the user account domain. The DBScheduler calculates the application assignment depending on this.

The option <Groups can be inherited> effects the inheritance of user account group memberships. For example, take an employee with a user account in an business role and once you have assigned groups to the business role, then the user account inherits the group assignments indirectly. Prerequisite for this is that the option <Groups can be inherited> is set for the user account. The inheritance of group memberships is described in the section How Active Directory User Accounts Inherit Active Directory Groups on page 285 in the Configuration Manual.

If an employee has several Active Directory user accounts, you can mark one of them as the prefered account.

If a user account is not required for a period of time, you can temporarily disable the user account by using the option <Account is deactivated>. If the user account is associated to an employee, you can control the behavior by disabling or deleting the employee. Refer to section Handling Disabling and Deletion of Employees and User Accounts on page 44. After the password has been entered wrongly several times (configuration dependent), the user account is locked in Active Directory. You can unlock the account using the task <Unlock account> in the Identity Manager.

The input <Exchange extension enabled> and <Exchange object is locked> are only displayed if Microsoft Exchange data is synchronized for the Active Directory user account. Refer to section Microsoft Exchange Recipients on page 276 for more information.

Password Data for Active Directory

Configuration Parameter for Setting up Password Data

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\Accounts\InitialPassword	Ínitial password as preset for new Active Directory user accounts.
TargetSystem\ADS\Accounts\InitialRandomPassword	When Active Directory user accounts are added a random generated passwort is created. The password has to contain a minimum of the character sets that are given in the sub-configuration parameters.
TargetSystem\ADS\Accounts\InitialRandomPassword\Character	This configuration parameter specifies whether a random generated password should contain at least one letter. If this configuration parameter is set, it has to contain at least one letter [a..z].
TargetSystem\ADS\Accounts\InitialRandomPassword\Length	This configuration parameter specifies how many characters the random generated password has.
TargetSystem\ADS\Accounts\InitialRandomPassword\Numeric	This configuration parameter specifies if the random generated password should contain at least one number. If the configuration parameter is set, it must contain at least one number [0...9].
TargetSystem\ADS\Accounts\InitialRandomPassword\SendTo	This configuration parameter specifies which employee the random generated password should be sent to (Cost center/department/location/Role manager, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the configuration parameter "TargetSystem\ADS\DefaultAddress".
TargetSystem\ADS\Accounts\InitialRandomPassword\SpecialCharacter	This configuration parameter specifies whether at least one special character should be included in the random generated password. If this configuration parameter is set, at least one special character must be included.
TargetSystem\ADS\Accounts\InitialRandomPassword\UpperCase	This configuration parameter specifies whether at least one capital letter should be included in the random generated password. If this configuration parameter is set, at least one capital [A..Z] must be included.
TargetSystem\ADS\Accounts\NotRequirePassword	Should the option ”No password necessary“ be activated for new Active Directory user account?.
QER\Person\UseCentralPassword	The employee’s central password is automatically mapped to the employee’s user account in all permitted target systems.

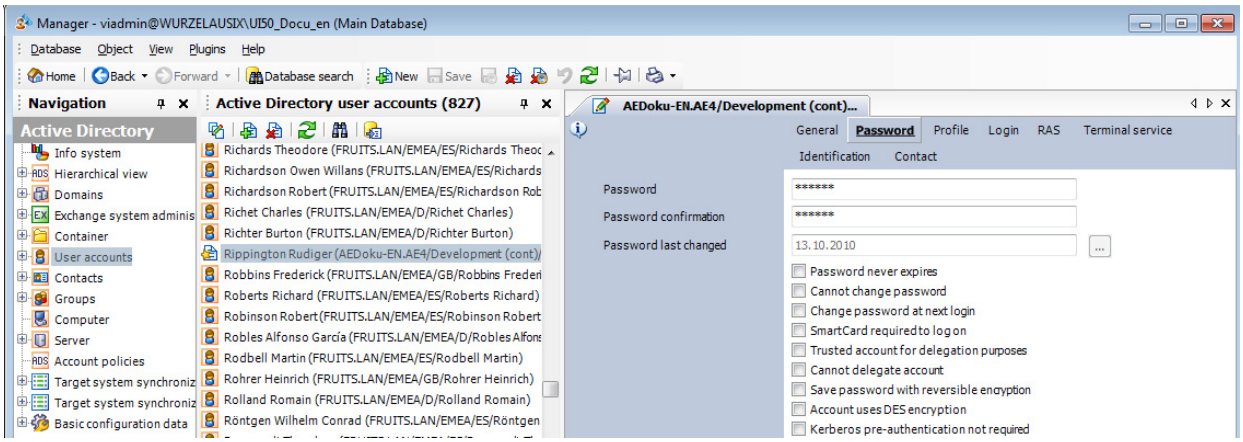
When an Active Directory user accounts are set up, the globally defined account policy and data for issuing passwords becomes valid. Apply these settings to the domain. Further information is available in the section Setting Up an Active Directory Domain on page 206. Use the form <Assign ADS Account policies> to define more policies for Active Directory domain with the fucntion level Windows Server 2008 R2.

Specify an initial password in the configuration parameter ”TargetSystem\ADS\Accounts\InitialPassword“ to be used for new users. Specify whether a random generated password should be initially issued when a new user account is added using the configuration parameter

"TargetSystem\ADS\Accounts\InitialRandomPassword". Use the subparameter to specify the character set that this password has to contain and specify to which employee the initial password should be sent by email. Depending on the configuration parameter "QER\Person\UseCentralPassword" the employee's central password can be mapped to the Active Directory user account's password.

Enter a password for the user on the <Password> tab. The date that the password was last changed is read from the Active Directory system and cannot be changed manually.

Password Data



Specify the following password options:

- Password never expires
  This option is usual used for service accounts. It overwrites the maximum lifetime of a password and the option <Change password at next logon>.

- Cannot change password
  This option is normally set for user accounts that are used by several users.

- Change password at next logon
  The user has to change the password the next time they log in.

- Save passwords with reversible encryption
  By default, passwords that are saved in Active Directory are encrypted. When you use this option, passwords are saved in plain text and can be restored again. If Apple users log into their Active Directory network, activate this option for the effected Active Directory user accounts.

You can define additional security relevant options:

- SmartCard required to log on
  Set this option to save public and private keys, passwords and other personal information for this Active Directory user account. In order to log onto the network the user's computer needs to be equipped with a Smartcard reader and the user needs to have a PIN (Personal Identification Number).

- Account trusted for delegation purposes
  Set this option so that a user can delegate the responsibility for administration and management of a partial domain to other user or another group.

- Cannot delegate account
  Set this option when this account may not be assigned for delegation purposes from another account.

- Account uses DES encryption
  Set this option when you want to activate DES (Data Encryption Standard).

- Kerberos pre-authentication not required
  Set this option when the account uses a different implementation of the Kerberos protocol.

Profile and Home Directories

Configuration Parameters for Setting Up User Directories

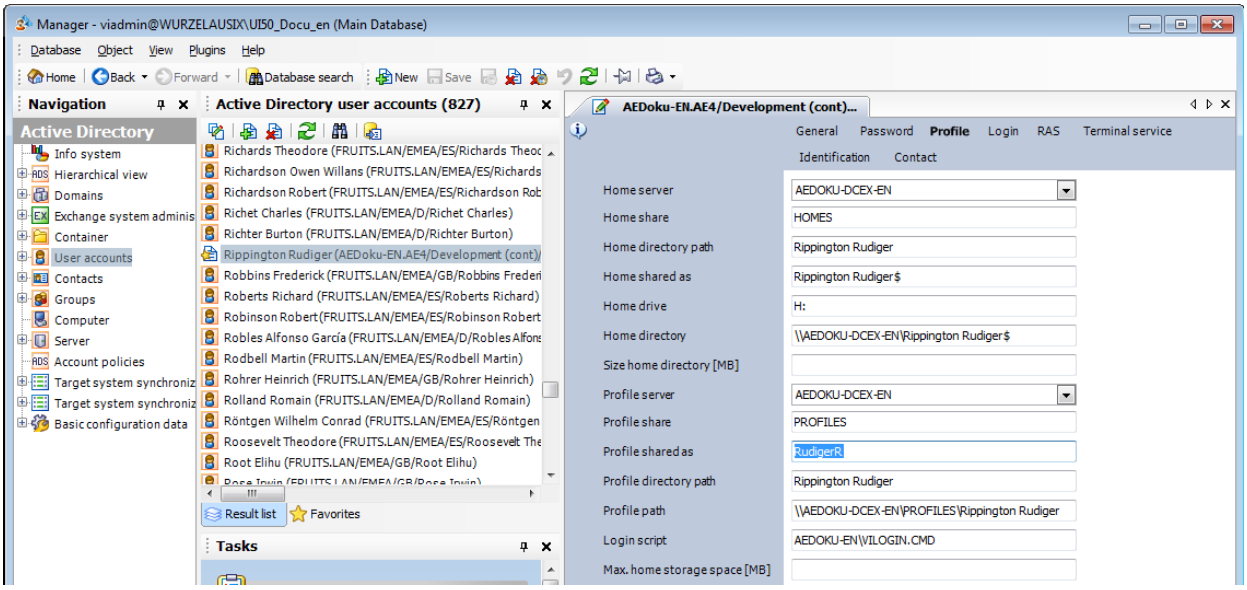
CONFIGURATION PARAMETER	MEANING
QER\Person\User\Access-Rights\HomeDir	Configures the access rights for user's home directory. In order to set user rights the configuration parameter and subparameters need to be set
QER\Person\User\AccessRights\HomeDir\EveryOne	This configuration parameter defines the rights for the user's home directory for everyone. Default: -r-w-x
QER\Person\User\Access-Rights\HomeDir\User	This configuration parameter defines the home directory user rights. Default: +r+w-x
QER\Person\User\Access-Rights\ProfileDir	Configures the access rights for a user's profile directory. In order to set user rights the configuration parameter and subparameters need to be set.
QER\Person\User\AccessRights\ProfileDir\EveryOne	This configuration parameter defines the 'EveryOne' rights for the a user's profile directory. Default: -r-w-x
QER\Person\User\Access-Rights\ProfileDir\User	This configuration parameter defines rights for the user's own profile directory. Default: +r+w-x
QER\Person\User\ConnectHome-Dir	The home directory that is connected when the user logs in.
QER\Person\User\PropertyMapping\ProfileFromHome	When home or profile directory is defined: Specifies whether the profile in the user's home should also be administrated.

On the <Profile> tab you can enter the data for the user's home and profile directories. The home and profile directories are determined from the company IT data for the assigned employee depending on the manage level of the user account

You can select the home server depending on the number of already existing (according to the database) home directories per home server. The given home directory is automatically added and shared by Identity Manager Service. To be fair to the special requirements of other network environments, a batch file can optionally be put aside that is created when a home directory is added. The final activation of the home directory can be made dependent on the results of executing this file. You can determine the size of the home directory over the scheduled task that is supplied by default "Load ADSAc-

count homesizes". This task can be customized in the Designer to meet your requirements. Read more in section Setting Up Scheduled Tasks on page 73.

Home and Profile Directory Data



When you enter a profile directory, a new user profile is created through Identity Manager Service that is loaded over the network when the user logs on. You can set the parameter "QER\Person\User\PropertyMapping\ProfileFromHome" to add a user profile. This ensures that the user profile is added in the users home directory.

You need set the configuration parameters „QER\Person\User\AccessRights\HomeDir" and „QER\Person\User\AccessRights\ProfileDir" and the subparameters and provide them with necessary values in order to ensure that access permissions are granted for the home and profile directories with Identity Manager Service.

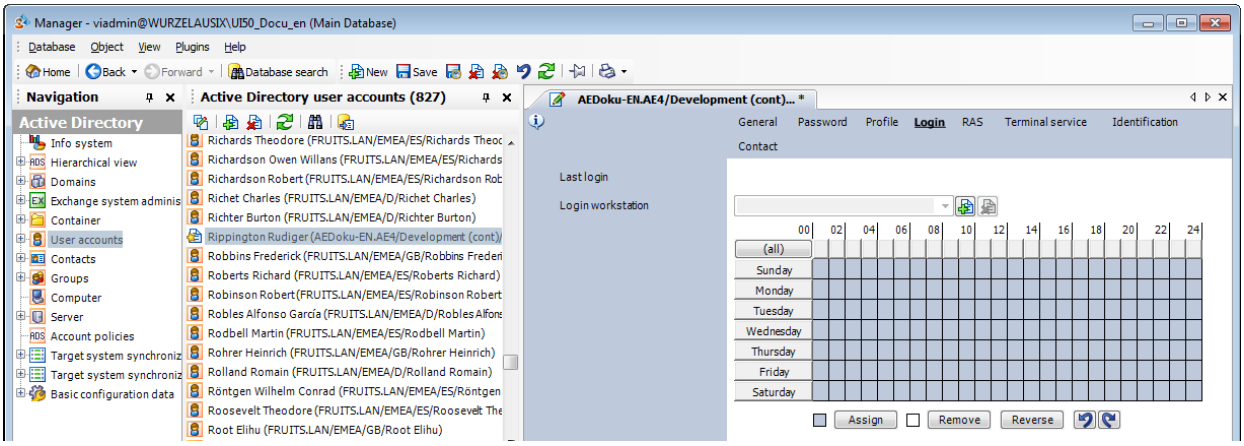
In certain circumstances it is necessary to store user account names such as "Administrators", "Everyone" or "Domain Users" as language dependent. The default language for user account names is english. You can enter new user account names with a translation in the category <Basic configuration data>\<User account names>.

In addition, you enter the login script name. If the login script is found in the login script subdirectory (usually Winnt\Sysvol\domain\scripts), you need to enter this subdirectory. The given login script is executed when the user logs in.

Active Directory User Account Login Data

On the <Login> tab, you specify the login data for an Active User user.

Specifying Login Options



The date of the last login is read in from the Active Directory system and cannot be changed manually.

By default, the user can log into any workstation. You can, however, define the workstations that the user can log into using the <Login workstation> form. Use the insert button next to the input field to activate it and add workstations. Use the delete button to remove workstations from the list.

Furthermore, you can specify how many days and hours a user may be logged in for. By default, logon is allowed at any hour and on each day of the week. The calendar shows a 7-day week, each box represents an hour. The configured login time are show in color respectively. If a box is filled out, login is permitted. If the box is „empty", login is not permitted. If a user is logged on, the logon is disconnected after the permitted login period is exceeded.

You can select a time period with the mouse or a key. User the <Assign> and <Remove> buttons to allow or not allow the selected time period for logging in. Use the <Reverse> button to invert the contents of the boxes in the selected time period. Use the arrow keys to resetor repeat a selection.

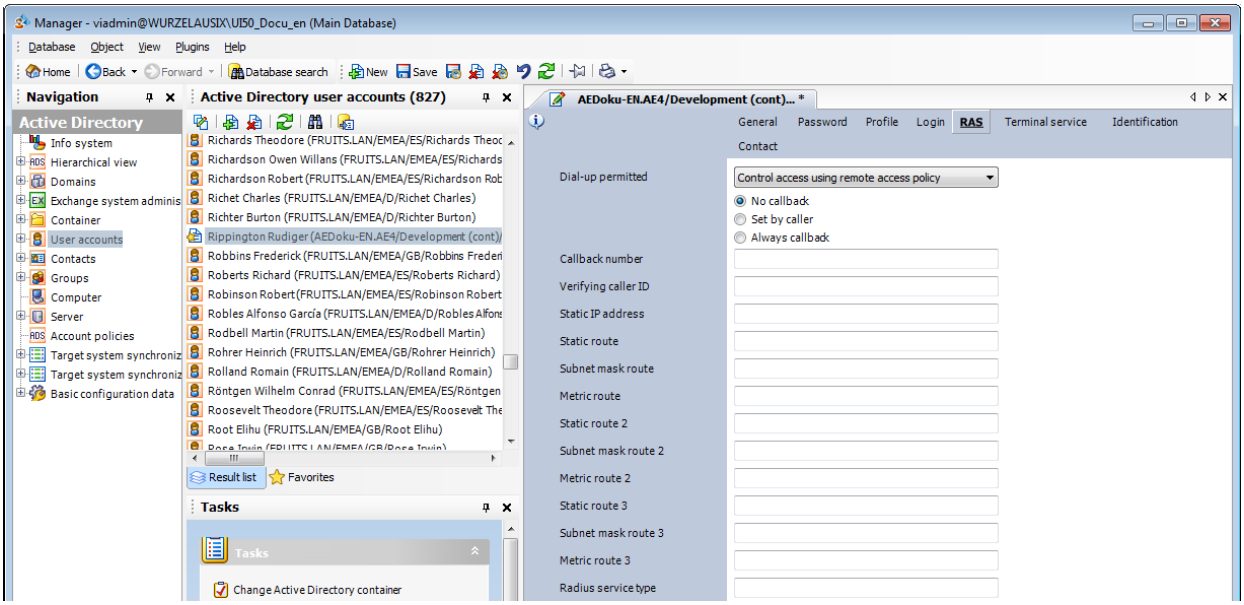
Remote Access Service Dial-in Permissions

Configuration Parameter for Remote Access Services Properties

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\EnableRAS	Maps Remote Access Service (RAS) properties of Active Directory user accounts. This is a preprocessor relevant parameter. The database needs to be recompiled after it has been changed.

On the <RAS> tab you can allocate remote dial-in permissions for the user in the network and specify the callback option.

Specify Dail-in Options



With dial-in permission you specify whether a user may dial into the network. The following are possible:

- Allow access
  This permits the user to dial into the network.

- Deny access
  With this users are not allowed to dial into the network.

- Control access through Remote Access Policy
  This data specifies that access to the network is controlled over RAS guidelines. RAS guidelines are usually used to apply the same access permissions to several users.

You can configure the following callback options:

- No callback
  The callback function is switched off by this option.

- Set by caller
  The server expects the user to input the number that he can be called back on.

- Always callback
  The server tries to call the user back over the given number.

The following data can be edited depending on the selected domain mode (mixed or native).

- Verifying caller ID
  If a user dials-in from a defined number in the network then enter the number here.

- Static IP address
  If a user is assigned a fixed IP address in the network, enter it here.

- Static routes with IP address, network address and metric
  If static route should be used for the dial-in connection, enter the IP addresses, network addresses and metrics for the target network.

Connection Data for a Terminal Server

Configuration Parameter for Terminal Server Properties

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\ADS\Terminal-Properties	Displays terminal properties for Active Directory user accounts. This is a preprocessor relevant parameter. The database needs to be recompiled after it has been changed.
QER\Person\User\Access-Rights\TerminalHomeDir	Configures the access rights for the user's teminal home directory. In order to set user rights, the configuration parameter and sub-parameters need to be set.
QER\Person\User\Access-Rights\TerminalHomeDir\Every-One	This configuration parameter defines the 'EveryOne' rights for a user's terminal home server. Default: -r-w-x
QER\Person\User\Access-Rights\TerminalHomeDir\User	This configuration parameter defines the rights for the user's own terminal home directory.Default:+r+w-x
QER\Person\User\Access-Rights\TerminalProfileDir	Configures the access rights for the user's terminal profile directory. In order to set user rights the configuration parameter and subparameters need to be set.
QER\Person\User\Access-Rights\TerminalProfileDir\Every-One	This configuration parameter defines the 'EveryOne' rights for a user's terminal profile directory. Default: -r-w-x
QER\Person\User\Access-Rights\TerminalProfileDir\User	This configuration parameter defines the rights of a user's own terminal profile directory. Default: +r+w-x

On the <Terminal service> tab, you enter the required data for adding a user profile that should be available to the Active Directory user account for logging onto a teminal server.

In order for a user to allow a user to log onto a terminal server you need to set the option <Login to terminal server permitted>. To specify a program that should be started when the terminal server is logged onto, enter the corresponding command line and working directory. If this data is inherited from the client, activate the option <Overwrite client configuration>.

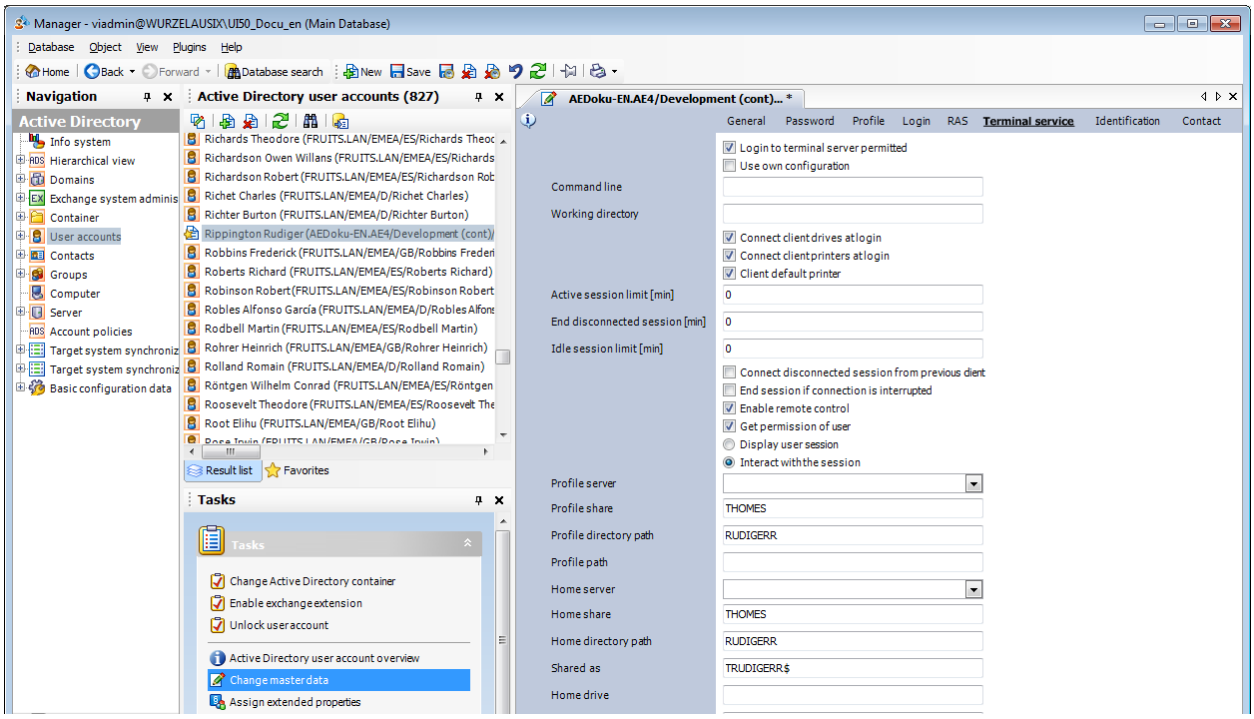
Specify whether client device connections should automatically be restored when logging onto a terminal server using the options <Connect client drives at logon>, <Connect client printer at logon>, <Client default printer>.

In addition, define a timeout setting for a terminal server connection. You can limit the maximum connection time with the input <Active session time [mins]>. After the time is exceeded the connection to the terminal server is detatched or ended. The field <End disconnected session [mins]> contains the time period that a disconnected connection is maintained. The field <Idle session limit [mins]> contains

the maximum time without client activity before the connection is detached or ended. If a connection is broken, you can specify if the session should be restored to a disconnected state and if a separate session from an arbitary client computer can be started.

The option <Activate remote control> specifies whether remote monitoring or control is activated for this session. You specify whether permission needs to be obtained for the user to monitor the session. Select the option <Display user session> if you wish to monitor the user session. If an option is selected with <Interact with session>, it means that the person monitoring can input data into the session over the keyboard or the mouse.

Data for Logging into a Terminal Server



You can set up a profile or home directory for a terminal server that is available after the user has logged onto the terminal server. A profile directory can be given that is available to the user to log on to a terminal server for a terminal server session. A home directory can be added on the terminal server in the same way. You can enable the configuration parameter ”QER\Person\User\PropertyMapping\ProfileFromHome“ to add a user profile. This ensures that the user profile is stored in the user’s home directory. The terminal home and profile servers are determined from the company IT data for the assigned employee depending on the manage level of the user account.

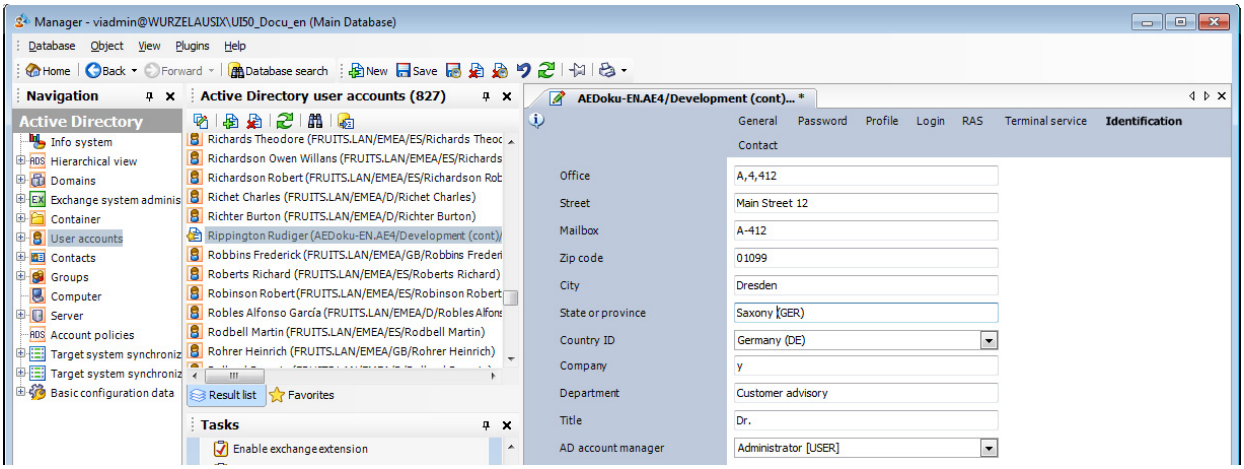
You need set the configuration parameters „QER\Person\User\AccessRights\HomeDir“ and „QER\Person\User\AccessRights\ProfileDir“ and the subparameters and provide them with necessary values in order to ensure that access permissions are granted for the home and profile directories with Identity Manager Service.

In certain circumstances it is necessary to store user account names such as ”Administrators“, ”Everyone“ or ”Domain Users“ as language dependent. The default language for user account names is english. You can enter new user account names with a translation in the category <Basic configuration data>\<User account names>

Further Identification Data

Enter the address information to contact the employee that uses this Active Directory user account. This data is determined from the assigned employee depending on the manage level of the user account. Apart from the address and country ID data, you can specify an ADS account manager.

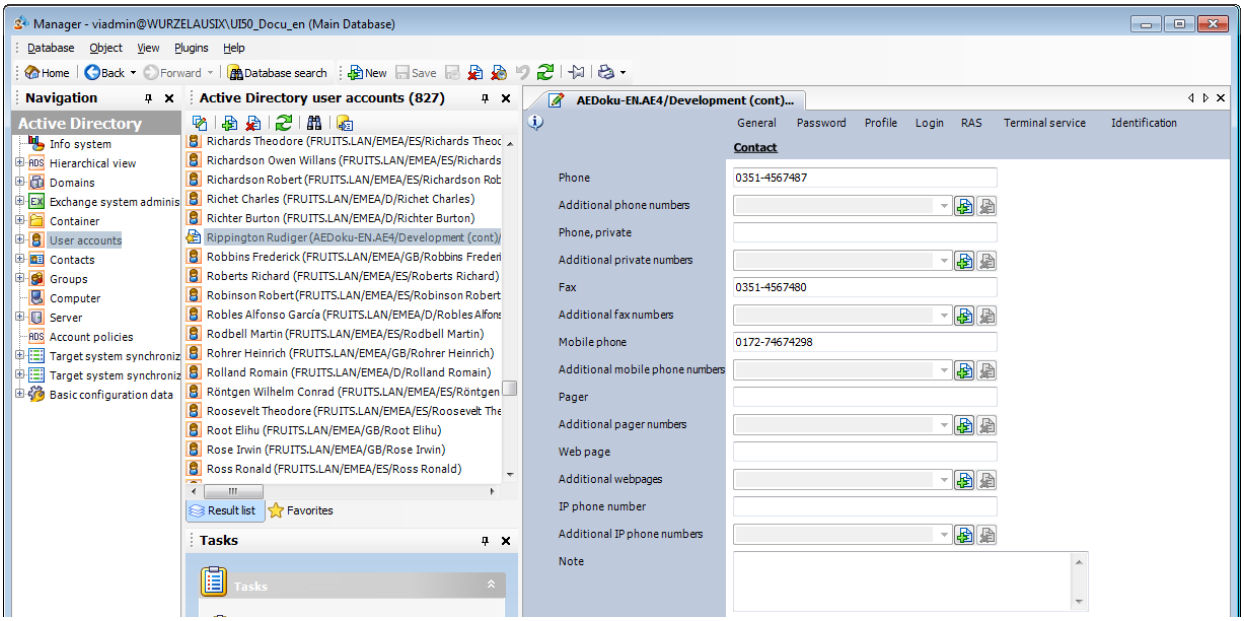
Address Data



Contact Data for an Active Directory User Account

Enter the data for contacting the Active Directory user account by telephone. This data is determined from the assigned employee depending on the manage level of the user account.

Telephone Data



Additional Tasks for Managing Active Directory User Accounts

After you have entered the user account master data, you can apply different tasks to the Active Directory user accounts. You can see the most important information about a user account on the overview form. The task view contains different forms with which you can run the following tasks.

Moving Active Directory User Accounts

To change (move) an Active Directory user, run the task <Change Active Directory container>. Active Directory user accounts can only be moved within an Active Directory domain.

Unlock Active Directory User Accounts

In Active Directory, if a user enters a wrong password more than once (depending on the configuration), the user is locked. You can unlock the Active Directory user account in the Identity Manager with the task <Unlock user account>.

Assign Active Directory Groups Direct to Active Directory User Accounts

All a user's Active Directory groups are shown on the overview form. Active Directory groups can be assigned directly or indirectly. Indirect assignment is executed by allocating the employee and the Active Directory groups to roles. If the employee has a user account, the Active Directory groups in the role are inherited by the user account. To react quickly to special requests, you can assign Active Directory groups directly to the user account. To do this you use the form <Assign groups>. See section Assigning Company Resources through Roles on page 78 for more information on group management.

Assign Extended Properties

Additional objects are meta objects that cannot be mapped directly in Identity Manager, for example, operating codes, cost codes or cost accounting areas. These extended properties are implemented in compliance rule testing. You can find out more about it by reading section Setting Up Extended Properties on page 424.

Edit Microsoft Exchange Settings for Active Directory User Accounts

The Active Directory user account's overview form shows mailboxes, email addresses and applicable restrictions on receiving. A description of how to configure a mailbox or an email address for an Active Directory user account can be found in section Microsoft Exchange Recipients on page 276.

Assign Account Policies for Active Directory User Accounts

It is possible to define more account policies to the default domain password policies for Active Directory domains with the "Windows Server 2008 R2" function level. This allows individual users and groups to be subjected to stricter account policies as intended for global groups. Use the task <Assign AD account policies> to assign account policies to Active Directory user accounts or to delete them. See section Account Policies for Active Directory Domains on page 255 for more information about setting up account policies.

Managing Active Directory User Accounts with User Account Resources

You can implement user account resources to automatically create Active Directory user accounts for company employees. You can set up user account resources for each domain in an Active Directory environment. The basic mechanisms are explained in the section Creating User Accounts with User Account Resources on page 37.

If an employee needs to obtain the user account through user account resources, the employee has to have a central user account and obtain the company IT data through assignment to a primary depart-

ment, primary location or a primary cost center. Refer to the section Handling Employees and User Accounts on page 30.

When a user account resource is assigned to an employee the default installation first checks if the employee already has a user account in the user account resource domain. If no user account exists, a new user account is created with the default manage level. If a user account does already exists and is deactivated, then it is unlocked. In this case, the user account manage level has to change in retrospect.

Creating a User Account Resource for an Active Directory Domain

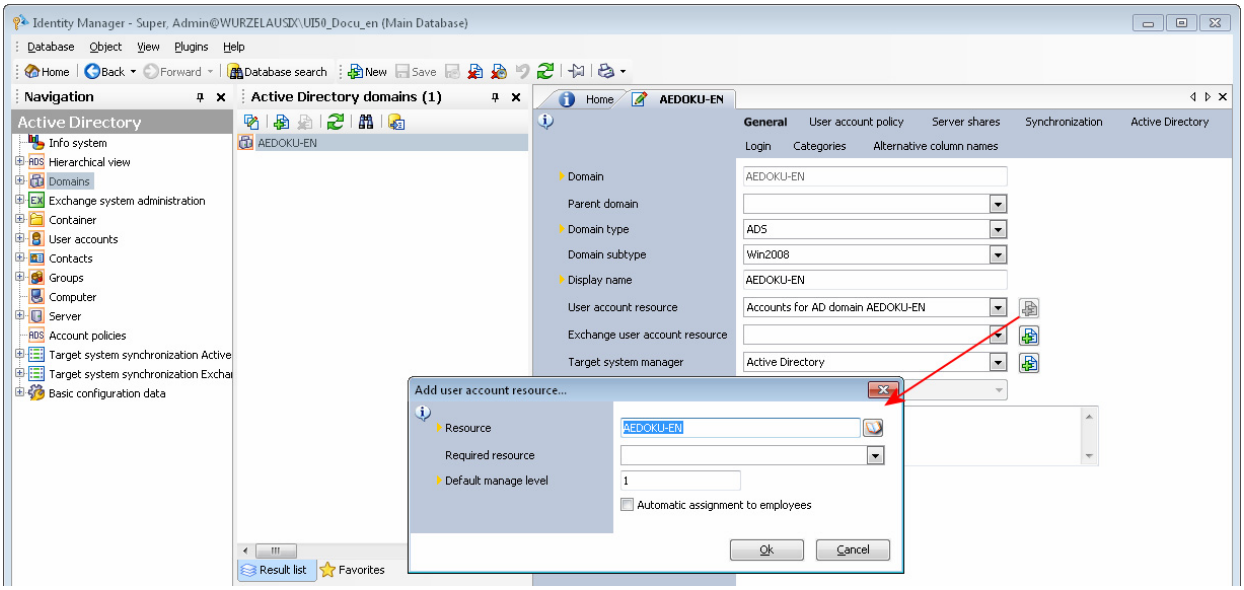
Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

Configuration Paramater for User Account Resources

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\UniqueDefaultManageLevel	When the parameter is set, a different default manage level is expected for each user account resource in the target system (default). If the parameter is not set, each user account resource in the target system may have the same default manage level.

You create user account resources for an Active Directory domain in the category <Active Directory Service>\<Domains>. Add a new user account resource on the domain form with the button next to the input field.

Creating a User Account Resource for an Active Directory Domain



Enter the following data for the user account resource:

- The resource identifier.

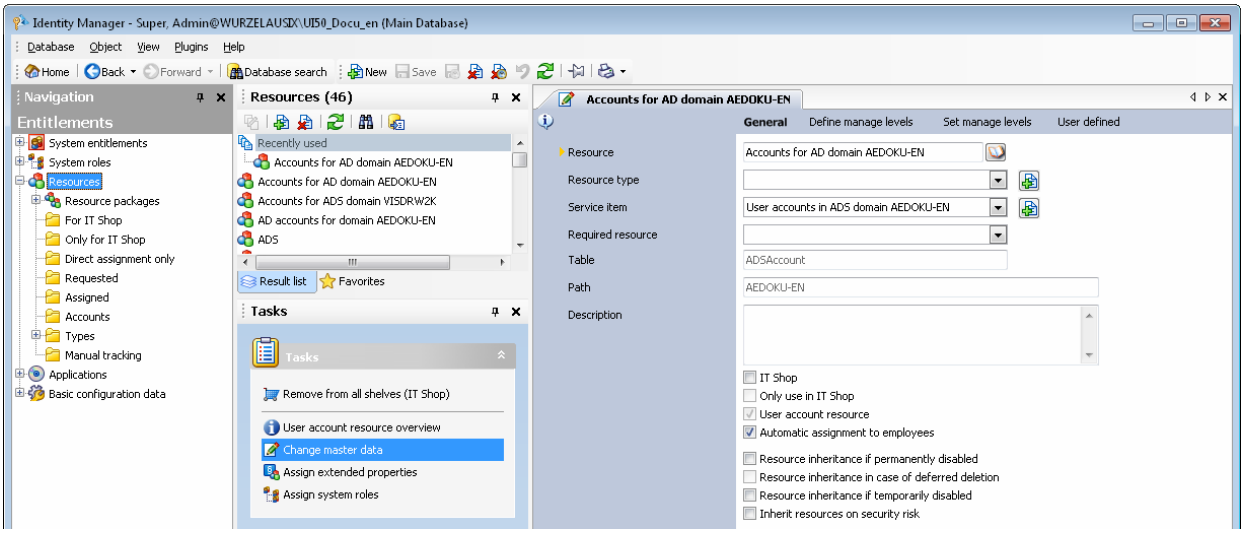
- Default manage level
  Specify the default manage level that will be used when a new user account is added using this user account resource. Enter the value ”1“ to create user accounts in the Identity Manager default installation with a manage level ”Full Managed“. Refer to section Manage Levels for Handling Active Directory User Accounts on page 237.

- Assumed resource.
  Here you can define dependencies between user account resources. This field is left empty for Active Directory domains.

- Automatic assignment to employees.
  Label the user account resource with this option when it should be automatically assigned to all internal employees. The user account is assigned to every employee tt is not marked as external on saving. The moment a new employee is added, they also are assigned this user account.The assignment is computed by the DBScheduler.

A new user account resource is created when the data is saved. Then, you can edit further data for this user account resource in the category <Entitlements>\<Resources> in the filter <Accounts>.

User Account Resource Post-processing



Addition user account resource data is:

- A resource type.
  Resources should obtain a resource type. This resource type defines future post-processing steps for resource requests or resource assignments. Without a resource type, manual post-processing of an request or assignment is not possible.

- Service Item
  Assign a service item to the user account resource or add a new one. This way the resource can be internally booked when the resource is requested.

- The base table in which the user accounts are displayed
  This data is preset with the table ”ADSAccount“ when a user account resource is assign to an Active Directory domain and cannot be edited.

- The domain path used by the user account resources
  This data is preset with the NetBIOS name of the Active Directory domain when a user account resource is assigned to an Active Directory domain and cannot be edited.

- Description
  Additional information about the user account resource.

- Specifying for use in the IT Shop
  Label a resource that can be requested through the IT Shop with the option <IT Shop>. This user account resource can be requested by employee via the web front-end and distributed using a defined authorization procedure. The user account resource can still be directly assigned to employees and roles outside the IT Shop. Set the option <Use only in IT Shop> so that the resource can only be requested through the IT Shop. In this case the user account resource can only be requested through the IT Shop.

- Options to deal with inheriting to disabled employees.
  You define the inheritance behavior for each user account resource yourself. The inheritance options of any possible predecessor resources are overwritten. You may want to an employee to inherit a user account resource to, for example, ensure that all required permissions are immediately reinstated for an employee that is reactivated at a later date. User resource account have the options <Resource inheritance if permanently disabled>, <Resource inheritance if temporarily disabled> and <No inheritance on security risk> for mapping inheritance behavior. If an employee does not continue to inherit the user account resource when disabled, the user account connected with the employee that was created from this resource assignment is deleted.

Manage Levels for Handling Active Directory User Accounts

You can specify the manage level for a user account resource for handling Active Directory user accounts. The user account's manage level determines the scope of the properties that a user account inherits from an employee. This means that an employee can have several user accounts in an Active Directory domain:

- Default user account that inherits all properities from the employee

- Administrative user account that is associated to an employee but should not inherit the properties from the employee.

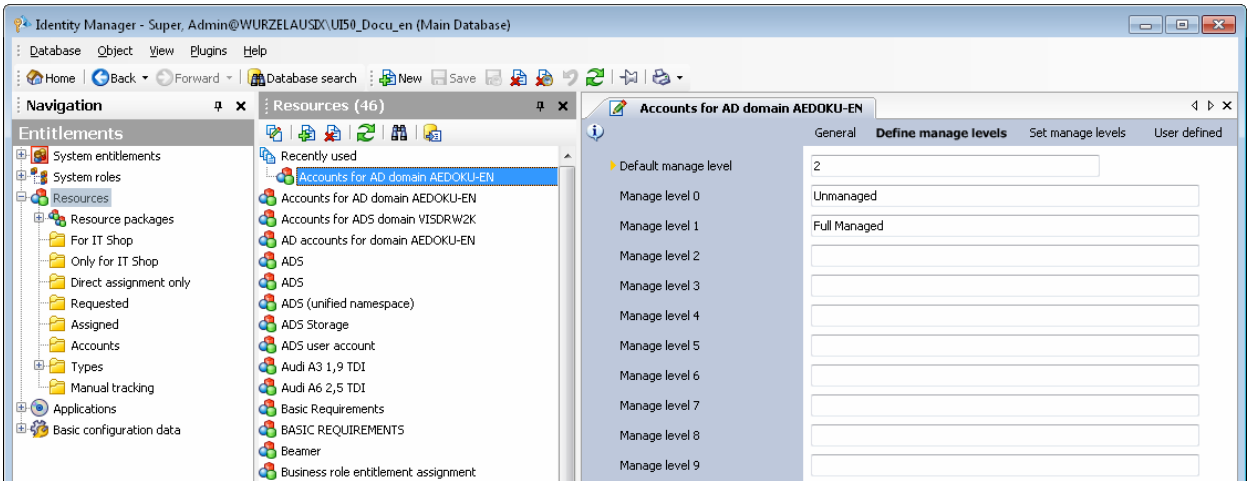
- Service account that contains the home directory and the profile directory of the employee but cannot inherit further properties.

The Identity Manager supplies a configuration for the manage level "Unmanaged" and the manage level "Full managed". User accounts with an manage level of "Unmanaged" are connected to an employee but do not inherit properties further properties. User accounts with an manage level of "Full managed" inherit specific properties from the assigned employee. These manage levels are taken into account in templates. You can define manage levels depending on your requirements. Then you need to extend your templates to include the methods for the addition manage levels.

The default manage level is used when new user accounts are added using this user account resource. If several Active Directory domains should be managed with these user account resources you have to create a separate user account resource for each domain. A different default manage level is expected for each target system user account resource in the default installation. However, the Identity Manager does allow several user account resources with the same default manage level to be used. The desired behavior can be controlled via the configuration parameter "TargetSystem\ADS\UniqueDefaultManage-

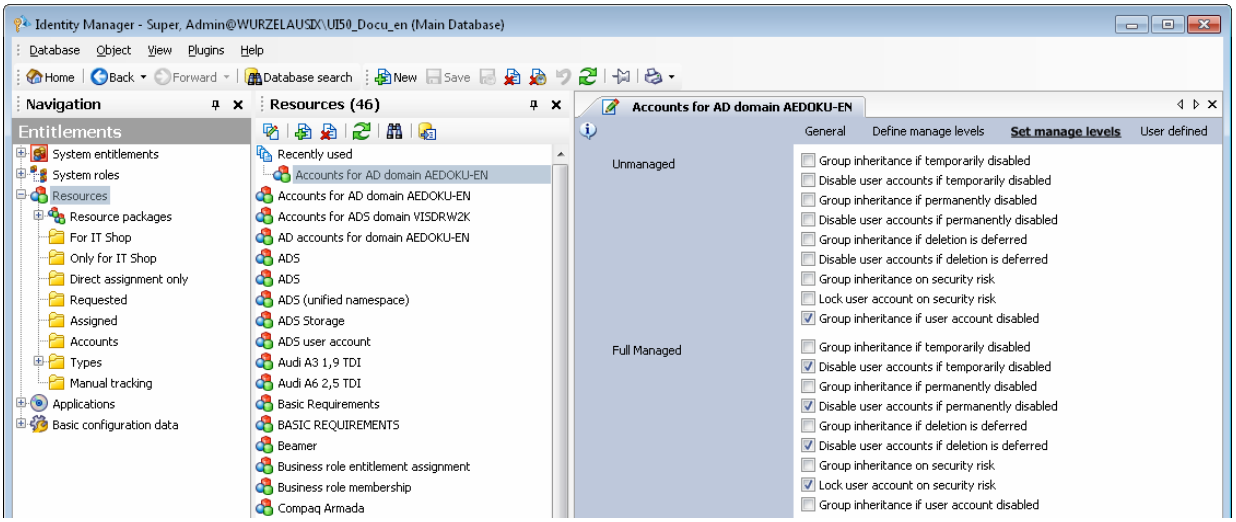
Level". There is a example in section Creating User Accounts with User Account Resources on page 37 for a more detailed explanation.

Manage Levels for an Active Directory Domain User Account Resources



Next, you can specify for each manage level, the effects on the user accounts and their group memberships of an employee being temporarily or permanently deactivated or deleted.

Edit User Account Resource Manage Levels



In order to remove authorization from an employee who has been disabled or deleted, you can disable the employee's user accounts. If the employee is reinstated at a later date, the user account are also reactivated. This behavior is controlled by the properties:

- User accounts if deactivated permanently
- User accounts if deactivated temporarily
- User accounts if deletion is deferred
- User accounts lock if security risk

The inheritance of group memberships can be defined for the target system of a user account resource. Inheritance can be discontinued if desired when, for example, the employee's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance procedures should be

applied to these employees. Existing group membership are deleted otherwise! This behavior is controlled by the properties:

- Group inheritance if deactivated permanently
- Group inheritance if deactivated temporarily
- Group inheritance if deletion is deferred
- Group inheritance if security risk

You can find more information in the section Handling Disabling and Deletion of Employees and User Accounts on page 44.

Deleting and Restoring Active Directory User Accounts

Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

Configuration Parameters for Deleting Users

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Person\User\DeleteDelay	This configuration parameter delays execution of a user account deletion. (-1 = delete immediately, otherwise = delete of value is exceeded (nx24)).
QER\Person\User\DeleteOptions	This configuration parameter to control behavior when users are deleted
QER\Person\User\DeleteOptions\FolderAnonymPre	If the delete options specify that a directory or a share should not be deleted, it is renamed and the given prefix is applied.
QER\Person\User\DeleteOptions\HomeDir	Deletes the user home directory.
QER\Person\User\DeleteOptions\HomeShare	Deletes the user home share.
QER\Person\User\DeleteOptions\ProfileDir	Deletes the user profile directory.
QER\Person\User\DeleteOptions\ProfileShare	Deletes the user profile share.
QER\Person\User\DeleteOptions\TerminalHomeDir	Deletes the user terminal home directory.
QER\Person\User\DeleteOptions\TerminalHomeShare	Deletes the user terminal home share.
QER\Person\User\DeleteOptions\TerminalProfileDir	Deletes the user terminal profile directory.
QER\Person\User\DeleteOptions\TerminalProfileShare	Delete the user terminal profile share.

Objects in Active Directory like Active Directory user accounts are issued with a unique identification number that is also linked to entitlements.

In the case of Active Directory domains with function level less than ”Windows Server 2008 R2“, IDs and connected entitlements are irreversibly lost when an Active Directory user account is deleted from Active Directory. This makes it difficult to restore Active Directory user accounts.

In the case of Active Directory domains with ”Windows Server 2008 R2“ function level or greater, you can delete Active Directory user accounts by dragging them to the Active Directory recycle bin. This moves the users to the recycle bin and from where they can be restored within a defined period without loss of IDs or entitlements.

Identity Manager uses various methods to delete Active Directory user accounts. When an Active Directory user account is deleted, the configuration parameters which handle user directories are taken into account.

Deleting without an Active Directory Recycle Bin

This method can be applied to all Active Directory domains that:

- do not have an Active Directory recycle bin because the function level is less that ”Windows Server 2008 R2“

or

- do not use the Active Directory recycle bin from ”Windows Server 2008 R2“ function level. Th Therefore the option <Use recycle bin> is not set for the Active Directory domain.

Once the security prompt has be confirmed, the Active Directory user account is marked for deletion in Identity Manager. The Active Directory user account is locked in Identity Manager and finally deleted from Active Directory and the Identity Manager database depending on the period set in the configuration parameter ”QER\Person\User\DeleteDelay“.

Deleting via the Active Directory Recycle Bin

This method is applied to Active Directory domain from ”Windows Server 2008 R2“ function level upwards, where the option <Use recycle bin> is set.

Once the security prompt has been confirmed, the Active Directory user account is marked for deletion in Identity Manager. The user account is immediately deleted in Active Directory. The Active Directory user account is locked in Identity Manager and once the retention time has expired it is finally deleted in the Identity Manager database. If there retention time has not been given then the value in the configuration parameter ”QER\Person\User\Delay“ is applied.

Restoring an Active Directory User Account

You can restore an Active Directory user account within the retention time via the context menu <Undo delete> independent of the method of deletion.

Active Directory Contacts

Configuration Parameters for Configuring Contacts

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\ADS\PersonAutoDefault	Automatic employee assignment for contacts that are created in the database takes place based on the given mode.
TargetSystem\ADS\PersonAutoFullsync	Automatic employee assignment for contacts that are created in the database through synchronization takes place based on the given mode.

A contact is a non-security principal. That means an Active Directory contact cannot log onto a domain. A contact for example, represents a user outside the company and is mainly used for distribution groups and email purposes.

The Identity Manager works with several methods to create contacts and to assign contacts to employees.

- Employees and contacts can be entered manually and assigned to one another.
- When a contact is added, an existing employee is assigned or created if necessary. In the process, the employee master data is created based on existing contacts. This procedure is, however, not the default procedure for the Identity Manager. The procedure is described in more detail in the section Automatic Assignment of Employees to User Accounts on page 40.

The basic mechanisms are dealt with in the chapter Employees and User Accounts on page 25.

Entering Master Data for Active Directory Contacts

Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

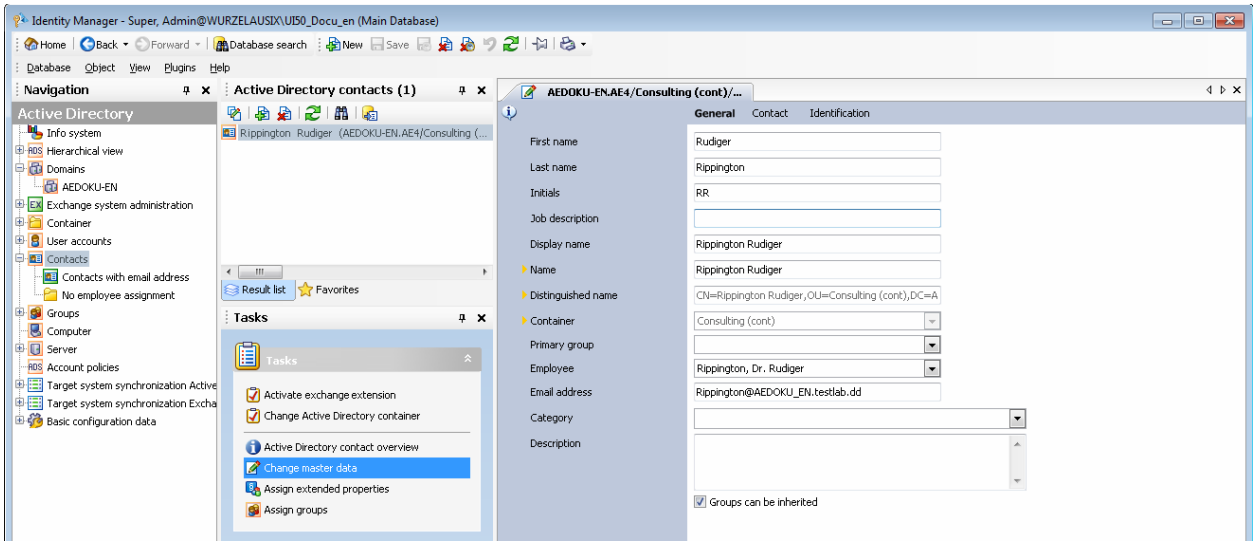
Active Directory contacts are displayed in the category <Active Directory Service>\<Contacts>. Enter the required data for an Active Directory contact on the <Change Master Data> form. Ensure that all the fields that are marked as compulsory are filled in.

General Master Data for Active Directory Contacts

Enter the general master data for the Active Directory contact, such as first name, last name and initials on the <General> tab. This data is used to format the display name and the contact's name.

Select the Active Directory container that the contact should be created in. The name for the contact is defined by a template when the Active Directory container is selected.

General Data



You can specify a primary group for the contact. Synchronization with the Active Directory environment assigns the contact to the group ”Domain users“ by default. Only Active Directory groups that are assigned to the contact are available as primary groups.

You can assign the contact to an employee. This can either be done through automatic employee assignment or by manual assignment. This method is explained in the section Automatic Assignment of Employees to User Accounts on page 40. You can also enter an email address and a detailed description for the contact.

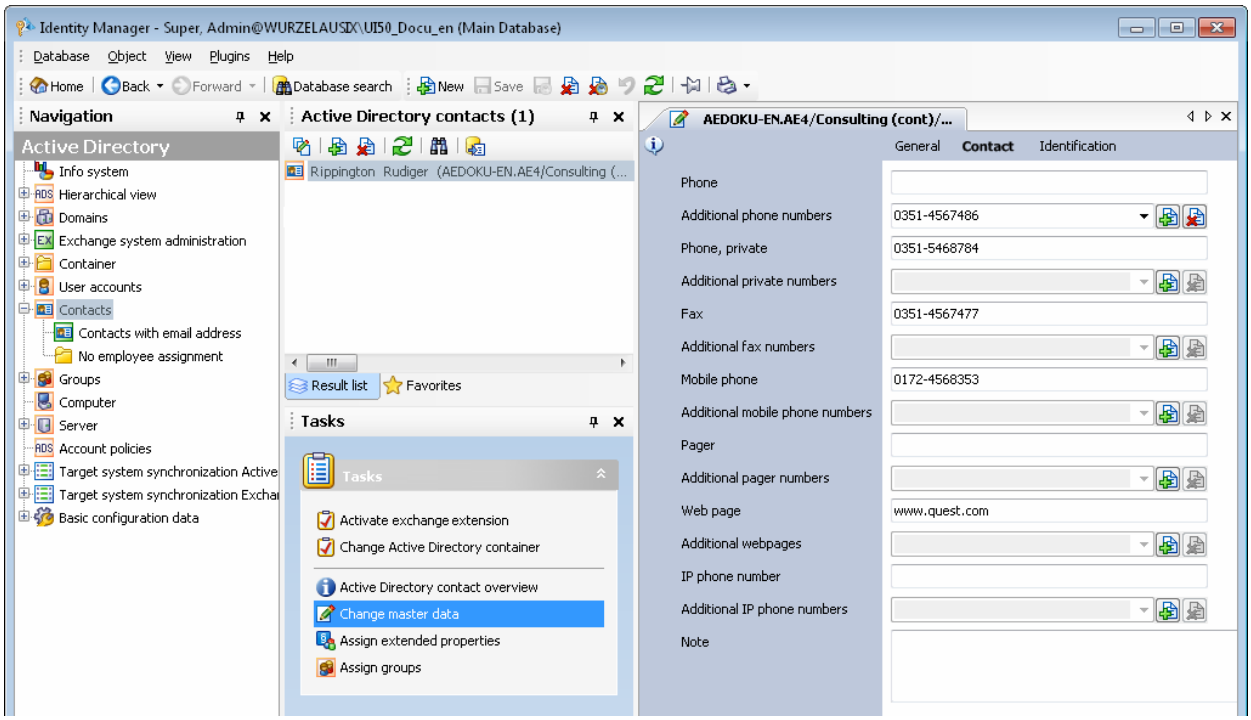
Categories are relevant for Active Directory contacts inheriting Active Directory groups. Active Directory contacts can selectively inherit Active Directory groups. To do this the contacts and groups are divided into categories. Use the pop-up menu <Category> to allocate one or more categories to the Active Directory contact. For more information read the section Inheriting Group Memberships Based on Categories on page 82.

The option <Groups can be inherited> effects the inheritance of Active Directory contact group memberships. For example, enter an employee with a Active Directory contact in an business role and once you have assigned groups to the business role, the user account inherits the group assignments indirectly. Prerequisite for this is that the option <Groups can be inherited> is set for the contact. The inheritance of group memberships is described in the Configuration Manual, section How Active Directory User Accounts Inherit Active Directory Groups on page 285.

Contact Data for an Active Directory Contact

Enter the telephone contact data for the employee uses the contact on the <Contact> tab e.g. telephone numberm fax, websites.

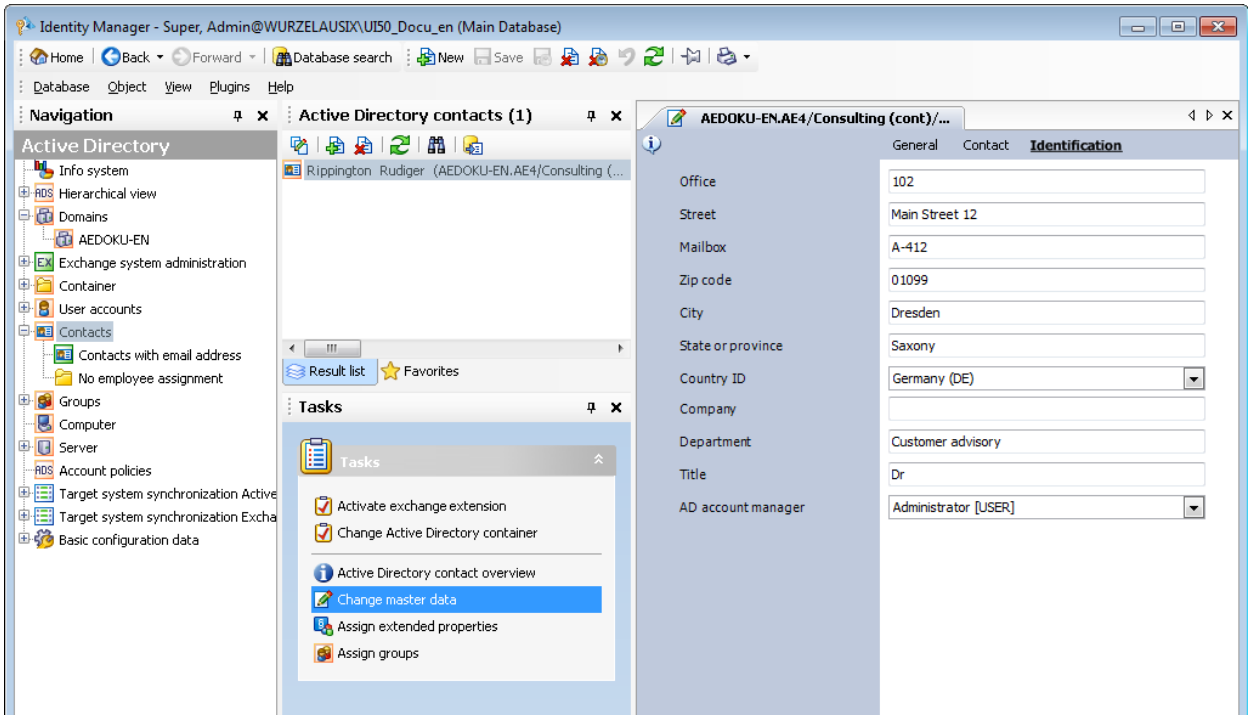
Contact Information



Further Identification Data

On the <Identification> tab enter the address information to contact the employee that uses this user account. Apart from the address and country ID data, you can specify an Active Directory account manager.

Address Data



Additional Tasks for Managing Active Directory Contacts

After you have entered the contact master data, you can apply different tasks to the Active Directory contacts. You can see the most important information about a contact on the overview form. The task view contains different forms with which you can run the following tasks.

Moving Active Directory Contacts

To change (move) an Active Directory contact, run the task <Change Active Directory container>. Active Directory contacts can only be moved within an Active Directory domain.

Assign Extended Properties

Additional objects are meta objects that cannot be mapped directly in Identity Manager, for example, operating codes, cost codes or cost accounting areas. These extended properties are implemented in compliance rule testing. You can find out more about it by reading section Setting Up Extended Properties on page 424.

Assign Active Directory Groups Directly to Active Directory Contacts

All Active Directory groups are displayed on the overview form for a contact. Active Directory groups can be assigned directly or indirectly. Indirect assignment is executed by allocating an employee and Active Directory groups to roles. If the employee has an Active Directory contact, the Active Directory groups in the role are inherited by this contact. To react quickly to special requests, you can assign Active Directory groups directly to the contact. To do this you use the task <Assign groups>. See section Assigning Company Resources through Roles on page 78 for more information on group management.

Edit Microsoft Exchange Settings for Active Directory User Accounts

The contact's overview form shows mailboxes, email addresses and applicable restrictions on receiving. A description of how to configure a mailbox or an email address for an Active Directory contact can be found in section Microsoft Exchange Recipients on page 276.

Deleting and Restoring an Active Directory Contact

Identity Manager uses various methods to delete Active Directory contacts. These are described in section Deleting and Restoring Active Directory User Accounts on page 239.

Active Directory Groups

Please read the online documentation for the Windows server you have in use for an explanation of group concepts under Active Directory.

In Active Directory, contacts, computers and groups can be collected into groups for which the access to resources can be regulated not only within a domain but across domains.

We distinguish between two group types:

- Security groups
  Authorizations are issued through security groups. Users, computers and other groups make up security groups and therefore, ease administration. Security groups are also used for email distibution groups.

- Distribution groups
  Distribution groups can be used as email distribution groups. Distribution groups do not have any security.

In addition, a group area is defined for each group type. Permitted group types are:

- Universal
  Groups in this scope are described as universal groups. Universal groups can be used to make cross-domain authorizations available.

- Domain local
  Groups in this scope are described as groups in the domain local groups. These groups are used when authorizations are issued within the same domain. Members of a domain local group can be users, computers or groups in any domain.

- Global
  Groups in this scope are described as global groups. Global groups can be used to make cross-domain authorizations available. Members of a global group are only users, computers and groups belonging to the global group's domain.

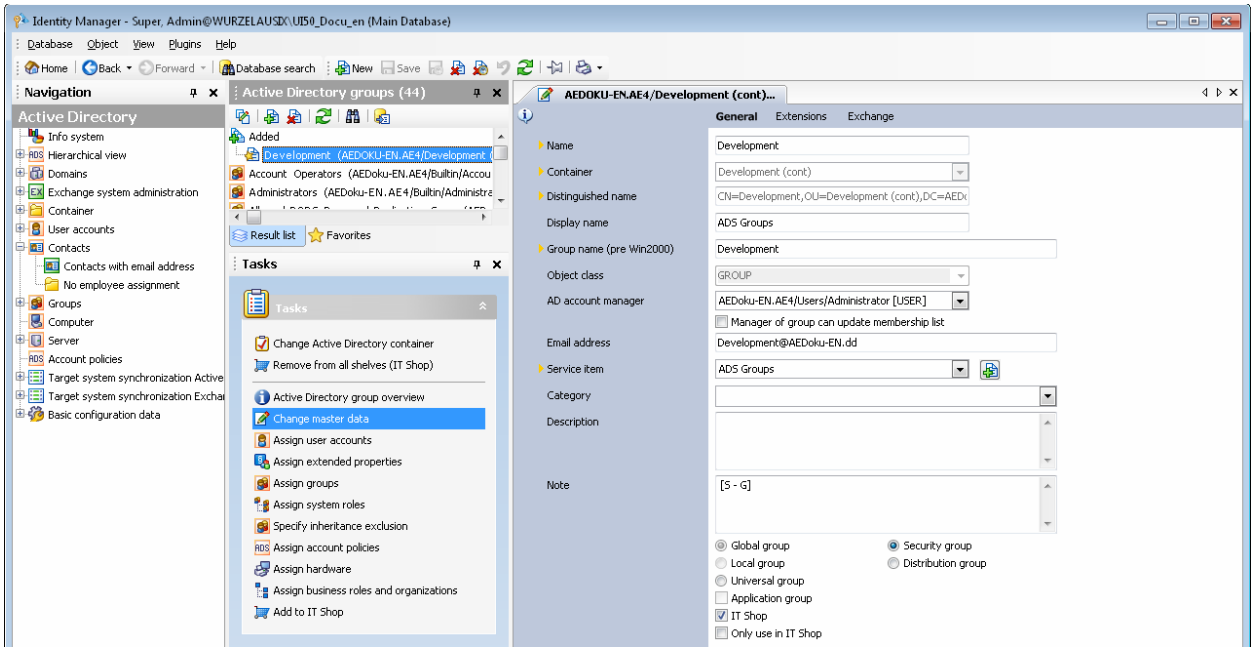
Different assignment to group scopes are possible depending on the domain mode (native or mixed).

Entering Master Data for Active Directory Groups

Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

Active Directory groups are displayed in the category <Active Directory Service>\<Groups>. Enter the required data for the Active Directory group on the form <Change master data>. Please ensure that all mandatory fields are filled out.

Active Directory Groups



Enter the following data for an Active Directory Group:

- Active Directory group display name
  The display name is used to display the group in the user interface.

- Active Directory goup name
  The group name for previous versions <group name (pre Win2000 is composed from the Active Directory group name.

- Active Directory container
  Select the Active Directory container that the group should be added to.

- Object class
  The object classes listed are the classes that are loaded from the Active Directory system into the database during synchronization. You can also enter object classes in to the input field. When a new group is added you can edit the object class. The object class cannot be changed after saving.

- Distinguished Name
  The distinguished name made up from the group and the Active Directory container and cannot be modified.

- Active Directory account manager with the option of edit permission for memberships in this group
  The option <Manager of group can update membership list> for Active Directory groups is only relevant if Microsoft Window Server 2003 is in use.

- Group email address

- Categories
  Active Directory groups can be selectively inherited by Active Directory user accounts and contacts. To do this, groups and users or contacts are divided into categories. Use the drop-down menu <Categories> to assign one or more categories to the Active Directory group. The principles of inheritance are explained in detail in section Inheriting Group Memberships Based on Categories on page 82.

- Description
  Detailed information about the Active Directory group.

- Group type and group scope
  Specify the group type (security group, distribution group) and the group scope (global, local, universal). Abbreviations for the combinations are copied to the input field <Note> and should not be modified there.

- Application group flag
  This option is automatically set when an application group is created and therefore, should not be manually edited. Special features of application group administration in the Active Directory environment can be found in the Configuration Manual in the section Managing Application Groups in Active Directory on page 286.

- IT Shop and service item
  A group that can be requested though the IT Shop is labeled with the option <IT Shop> (see Chapter Setting Up an IT Shop Solution on page 15. This group can be requested over the web interface from the company employees and issued through a defined approval procedure. However, the group can still be directly assigned to user accounts and roles outside the IT Shop. In order to avoid direct assignment, activate the option <Only use in IT Shop>. In this case groups can only be requested through the IT Shop.
  In order to use a group within the IT Shop, assign an additional service item to it or add a new service item. This allows the group to be booked internally.

Validity of Group Memberships

There are different assignments to Active Directory groups possible depending on the construction of the domain structure, the domain mode (single or mixed) and the domain trusts. You can find more exact information about permitted group memberships in the documentation for your Microsoft Windows server.

Ensure the following if you want to map group memberships via forests:

- The trusted domains are known.
  For more information, read section Trusted Domains on page 212.

- The name of the forest is entered in the <Forest> input field for the Active Directory domain.
  For more information, see section Active Directory Specific Master Data on page 210.

In the following tables the user and group memberships permitted in Identity Manager listed in Active Directory groups.

Group Memberships Permitted within a Domain

User and Contact Assignments to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP	
			USER	CONTACT
Mixed	Global	security	•	•
	Local		•	•
	Universal			
	Global	distribution	•	•
	Local		•	•
	Universal		•	•
Unified	Global	security	•	•
	Local		•	•
	Universal		•	•
	Global	distribution	•	•
	Local		•	•
	Universal		•	•

Group Assignments to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP					
			SECURITY			DISTRIBUTION		
			GLOBAL	LOCAL	UNIVER-SAL	GLOBAL	LOCAL	UNIVER-SAL
Mixed	Global	security						
	Local		•			•		•
	Universal							
	Global	distribution	•			•		
	Local		•	•		•	•	•
	Universal		•			•		•
Unified	Global	security	•			•		
	Local		•	•	•	•	•	•
	Universal		•		•	•		•
	Global	distribution	•			•		
	Local		•	•	•	•	•	•
	Universal		•		•	•		•

Group Memberships Permitted within a Hierarchical Domain Structure

User and Contact Assignment to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP			
			MIXED DOMAINS		UNIFIED DOMAINS	
			USER	CONTACT	USER	CONTACT
Mixed	Global	security		•		•
	Local		•	•	•	•
	Universal					
	Global	distribution		•	•	•
	Local		•	•	•	•
	Universal		•	•	•	•
Unified	Global	security		•		•
	Local		•	•	•	•
	Universal				•	•
	Global	distribution		•		•
	Local		•	•	•	•
	Universal		•	•	•	•

Group Assignments to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP					
			SECURITY			DISTRIBUTION		
			GLOBAL	LOCAL	UNIVER-SAL	GLOBAL	LOCAL	UNIVER-SAL
Mixed	Global	security						
	Local		•			•		
	Universal							
	Global	distribution						
	Local		•		•	•		•
	Universal		•		•	•		•
Unified	Global	security						
	Local		•		•	•		•
	Universal		•		•	•		•
	Global	distribution						
	Local		•		•	•		•
	Universal		•		•	•		•

Group Memberships Permitted within a Forest

User and Contact Assignments to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP			
			MIXED DOMAINS		UNIFIED DOMAINS	
			USER	CONTACT	USER	CONTACT
Mixed	Global	security				
	Local		•		•	
	Universal					
	Global	distribution				
	Local		•		•	
	Universal					
Unified	Global	security				
	Local		•		•	
	Universal					
	Global	distribution				
	Local		•		•	
	Universal					

Group Assignments to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP					
			SECURITY			DISTRIBUTION		
			GLOBAL	LOCAL	UNIVER-SAL	GLOBAL	LOCAL	UNIVER-SAL
Mixed	Global	security						
	Local		•		•	•		•
	Universal		•		•	•		•
	Global	distribution						
	Local		•		•	•		•
	Universal		•		•	•		•
Unified	Global	security						
	Local		•		•	•		•
	Universal		•		•	•		•
	Global	distribution						
	Local		•		•	•		•
	Universal		•		•	•		•

Group Memberships Permitted between Forests

User and Contact Assignments to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP			
			MIXED DOMAINS		UNIFIED DOMAINS	
			USER	CONTACT	USER	CONTACT
Mixed	Global	security				
	Local		•		•	
	Universal		•		•	
	Global	distribution				
	Local		•		•	
	Universal		•			
Unified	Global	security			•	
	Local		•		•	
	Universal		•			
	Global	distribution				
	Local		•		•	
	Universal		•		•	

Group Assignments to Groups

DOMAIN MODE	TARGET GROUP		MEMBER IN TARGET GROUP					
			SECURITY			DISTRIBUTION		
			GLOBAL	LOCAL	UNIVER-SAL	GLOBAL	LOCAL	UNIVER-SAL
Mixed	Global	security						
	Local		•		•	•		•
	Universal							
	Global	distribution						
	Local		•		•	•		•
	Universal							
Unified	Global	security						
	Local		•		•	•		•
	Universal							
	Global	distribution						
	Local		•		•	•		•
	Universal							

Additional Tasks for Managing Active Directory Groups

After you have entered the group master data, you can apply different tasks to the Active Directory group. You can see the most important information about a group on the overview form. The task view contains different forms with which you can run the following tasks.

Moving Active Directory Groups

To change (move) an Active Directory group, run the task <Change Active Directory container>. Active Directory groups can only be moved within an Active Directory domain.

Assign Active Directory Groups to Company Structures

It is possible for an user accounts and hardware to inherit a group if an Active Directory group is assigned to individual company structures. Active Directory groups are added to departments, cost centers, locations or business roles. If an employee is added to one of these company structures and this employee has a user account where the <Groups can be inherited> option set, then is account becomes member of the Active Directory group. You can find further information in the section Assigning Company Resources through Roles on page 78.

Inheritance processes are calculated by the DBScheduler. Group inheritance is described in the section How Active Directory User Accounts Inherit Active Directory Groups on page 285 in the Configuration Manual. Because Active Directory on supports a limited number of group members, a mechanism has been implemented to monitor memberships. Read the section Managing Application Groups in Active Directory on page 286 in the Configuration Manual for more information.

Add Users and Groups directly to Active Directory Groups

Use the tasks <Assign user> and <Assign groups> to assign an Active Directory group directly to Active Directory user accounts and other Active Directory groups. Note the characteristics described in the section Validity of Group Memberships on page 247 in particular.

Add Active Directory Groups to System Roles

Use the task <Assign system roles> to add Active Directory groups to system roles. If you assign a system role to employees, the groups are inherited by all the Active Directory user accounts that thie employees have. Active Directory groups with the option <Only use in IT Shop> set can only be assigned to system roles that also have this option set. See section System Roles on page 114 for more information.

Established inheritance mechanisms and calculation of system role assignments by the DBScheduler is described in detail in the Configuration Manual in section System Role Inheritance on page 283.

Specify Dependencies between Active Directory Groups

Use the task <Specify inheritance exclusion> to define dependencies between Active Directory groups. Enable this functionality with the configuration parameter ”QER\Structures\Inhertite\GroupExclusion“. By defining dependencies between the groups, the number of resulting memberships of Active Directory user accounts is reduced in the Active Directory groups. Read more in section Inheritance Exclusion on page 80

Assign Extended Properties to Active Directory Groups

Extended properties are meta objects for which there is no direct mapping, such as accounting codes, controlling areas or cost center areas, in the Identity Manager data model. These extended properties are used to check rule conformity. Use the form <Assign extended properties> to add extende properties. For more information see section Setting Up Extended Properties on page 424.

Assign Account Policies to Active Directory Groups

It is possible to define more account policies to the default domain password policies for Active Directory domains with the ”Windows Server 2008 R2“ function level. This allows individual users and groups to be subjected to stricter account policies as intended for global groups. Use the task <Assign AD account policies> to assign account policies to Active Directory groups or to delete them.

Assign Account Policies to Active Directory User Accounts

It is possible to define more account policies to the default domain password policies for Active Directory domains with the ”Windows Server 2008 R2“ function level. This allows individual users and groups to be subjected to stricter account policies as intended for global groups. Use the task <Assign AD account policies> to assign account policies to Active Directory user accounts or to delete them. See section Account Policies for Active Directory Domains on page 255 for more information about setting up account policies.

Edit Microsoft Exchange Settings for Active Directory Groups

The exchange relevent properties that are required for Active Directory groups that are going to used as distribution groups are displayed on the overview form. Refer to section Mail-enabled Groups on page 291 for setting up a distribution group.

Add Active Directory Groups to IT Shop

Tools: Identity Manager with application role <IT Shop>\<Administrators>; Manager

When Active Directory groups are assigned to an IT Shop shelf the groups can be requested by the shop’s customers. To ensure the group is requestable there are further prerequisites need to be guaranteed. There is more information about this in the section Requestable Products on page 33. To remove a Active Directory group from the IT Shop, use the task <Remove from all shelves (IT Shop)>.

Deleting Active Directory Groups

Once the security prompt has been confirmed, the Active Directory goup is marked for deletion in Identity Manager. The group is finally deleted from the Identity Manager database and the Active Directory system by Identity Manager Service.

Reports about Active Directory Groups

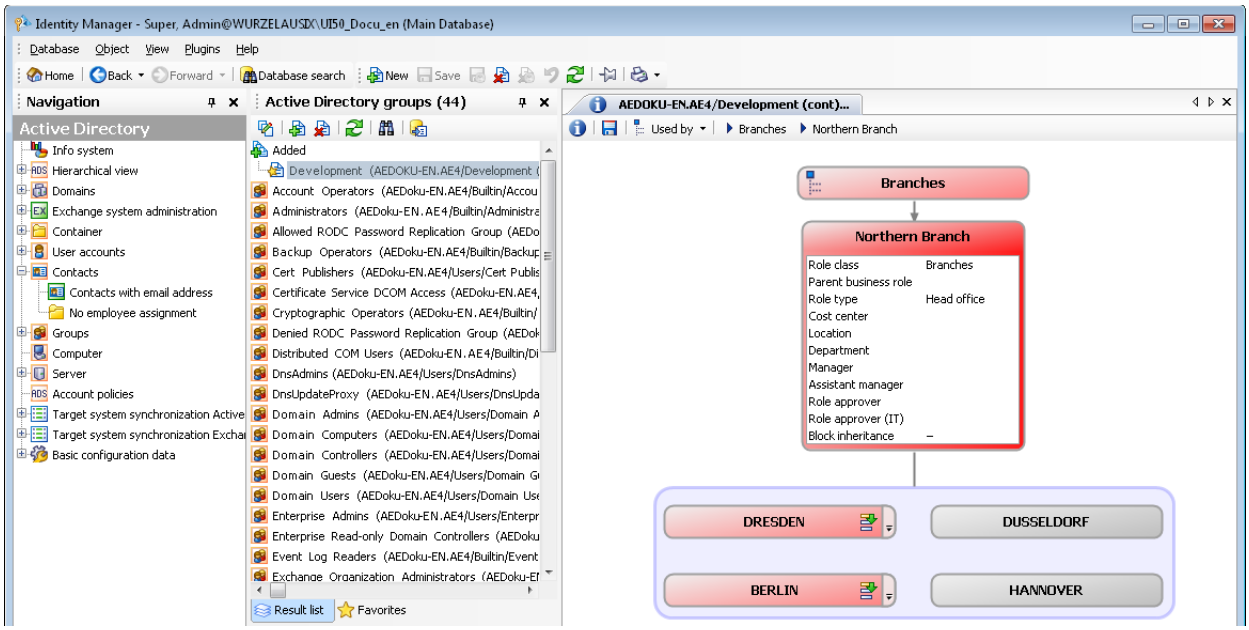
Identity Manager provides several reports that prepares information about the selected base object and its relations to other objects in the Identity Manager database. The following reports are available for Active Directory groups.

Overview of all Assignments

This report shows all employees that are assigned at least one Active Directory user account in the selected Active Directory domain. In this case, directly assigned objects are taken into account as well as

objects obtained via inheritance. The report shows which roles of a role class the employee belongs to. What you get is an organigram of the different role classes for the selected Active Directory group.

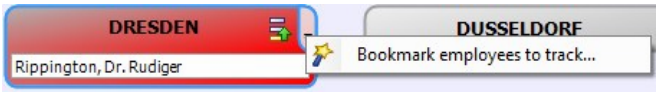
Report "Overview of all Assignments" for an Active Directory Group



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that violate the role and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

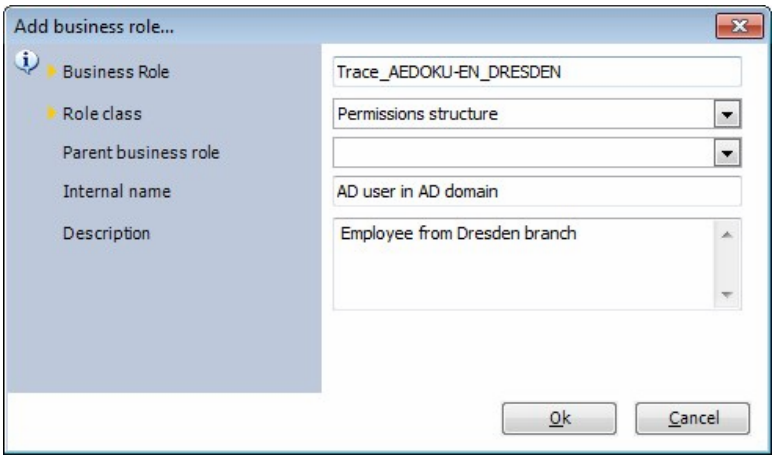
Bookmark Employee for Tracking



To do this, a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Account Policies for Active Directory Domains

It is possible to define serveral account policies for Active Directory domains with ”Window Server 2008 R2“ function level. This allows individual users and groups to be subjected to stricter account policies as intended for global groups. Read the documentation from the Window Server you use for more information about the concept of fine-grained password policies under Active Directory.

Entering Account Policies

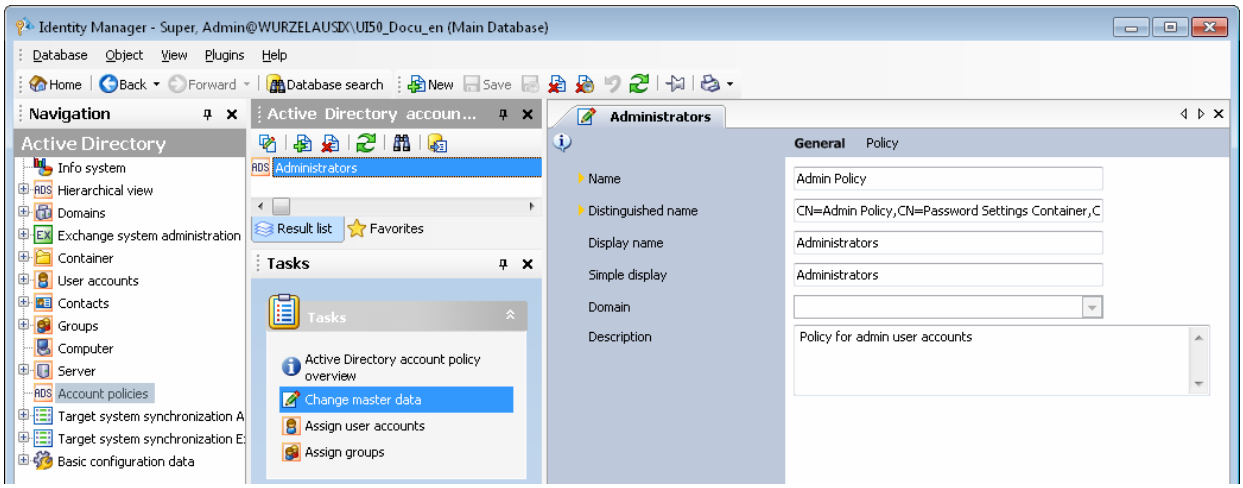
Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

Active Directory account policies are displayed in the category <Active Directory>\<AD account policies>. Account policies are loaded into the Identity Manager database during synchronization. You have the option to edit existing account policies and add new ones. Enter the required data for the Active Directory account policy on the <Change master data> from. Please ensure that you fill out all the mandatory fields.

General Master Data for an Account Policy

Enter general master data for an Active Directory account policy on the <General> tab.

Setting Up an Active Directory Account Policy



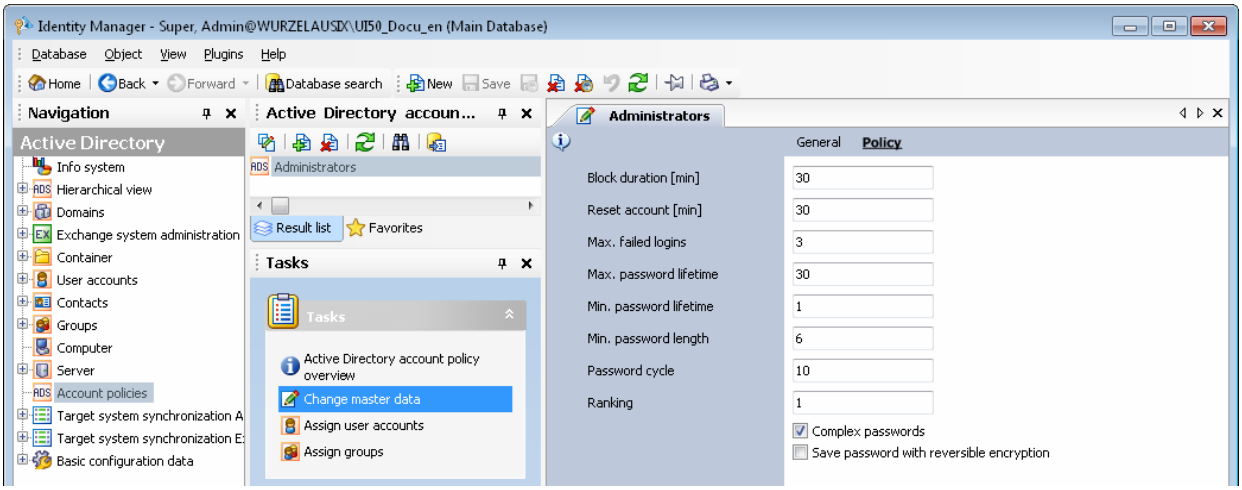
The following information is displayed for the Active Directory account policy:

- Account policy name
- Distinguished name
  The distinguished name made up from the account policy name, the system container for password policies ”Password Settings Container“ and the Active Directory domain.
- Display name for use in the user interface
- Simple display name
  The simple display name is used by systems that cannot interpret all the characters of the normal display name.
- Active Directory domain that account policy is available for.
- Description
  Detailed description of the account policy.

How to Define a Policy

Enter the settings for the policy on the <Policies> tab.

Setting for Active Directory Account Policies



The account policies include:

- Duration of block in minutes
  Enter the time period the the account should be locked for before it is automatically reset.

- Delay in minutes before account is blocked
  Enter the time period that can elapse between two invalid attempts to enter a password before a user account is blocked.

- The maximum number of incorrect password attempts
  Set the number of invalid passwords. If the user has reached this number the user account is blocked.

- The maximum lifetime of a password
  Enter the length of time a password can be used before a new password has to be set.

- The minimum lifetime time of a password
  Enter the length of time a password has to be used before the user is allowed to change it.

- Minimal length of the password
  Enter the minimum number of characters the password has to have.

- Password cycle
  Enter the number of new passwords to be saved. If the value 10 is entered, for example, The last 10 password for the user are saved.

- Ranking for password settings
  If several account polices are assigned to a user or a group, the account policy is used that has the lowest value.

- Complex passwords
  Use this option to specify that a password has to be complex.

- Save passwords with reversible encryption
  By default, passwords that are saved in Active Directory are encrypted. When you use this option, passwords are saved in plain text and can be restored again. If Apple users log into their Active Directory network, activate this option for the effected Active Directory user accounts.

Assigning Account Policies to Users

Use the form <Assign AD users> and <Assign AD groups> to assign account policies to single Active Directory user accounts or to Active Directory groups. If several account policies are assigned to one Active Directory user account, the actual account policy is found using specific rules. If there are no special account policy the Active Directory domain setting apply. Please refer to your Windows server documentation on fine-grained account policies under Active Directory for information about the rules for calculating this.

Setting Up Synchronization with a Microsoft Exchange Environment

Identity Manager Service takes care of reconciling the data between the Identity Manager database and the Microsoft Exchange environment. Prerequisites for synchronization are:

- The installation and configuration of a synchronization server
- Setting up the database for synchronization

The basic synchronization mechanisms are explained in the chapter Data Synchronization in Identity Manager on page 161.

Installation and Configuration of a Microsoft Exchange Synchronization Server

Access to a Microsoft Exchange server on the one hand and Active Directory on the other must be guaranteed in order to synchronize data between a Microsoft Exchange system and the Identity Manager database.

The synchronization server for Microsoft Exchange Server 2000, Microsoft Exchange Server 2003 and Microsoft Exchange Server 2007 and should ideally be an Active Directory server with an Microsoft Exchange server. A member server with Microsoft Exchange Server Management Tools is also supported as sychronization server. From Microsoft Exchange Server 2010 onwards, the synchronization server has to be a Microsoft Exchange server.

A server is required for setting up synchronization with a Microsoft Exchange environment that has the following software installed:

- Windows 2000 Server or Advanced Server mit mindestens Service Pack 2 for Windows 2000, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 or Windows Server 2008 R2
- Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, Microsoft Exchange Server 2010
- Microsoft .NET Framework at least Version 2.0
- Microsoft Software Installation (MSI) service

- If an Oracle database is used, Oracle Client Tools need to be installed in order to access the database.

- Installation of Identity Manager Service from the Setup-CD
  The installation is described in the section Installing Identity Manager Tools on page 23. Please take into account the advice for installation on a terminal server (see Installing on a Microsoft Windows Terminal Server on page 25).

Then you can configure Identity Manager Service on the synchronization server and start the service. Read the section Setting Up a Server for Database Access on page 44 in the Getting Started manual for more information.

If the server that performs the synchronization does not have a direct connection to the Identity Manager database, synchronization is aborted and a message is displayed. Ensire that a direct connection to the Identity Manager database is possible!

Necessary Identity Manager Service Access Rights to Synchronize with a Microsoft Exchange Environment

The Identity Manager Service user account, along with the groups ”Domain Admins“ and ”Enterprise Admins“ should have write access to the Active Directory schema. If security settings automatically inherited through Active Directory are not to be used in Microsoft Exchange, then you need to ensure that the user accounts in use have full access rights to the Microsoft Exchange objects ”Administrative groups“, ”Global address lists“, ”Offline address lists“, ”Server“, ”Storage groups“, ”mailbox store“, ”Folder“ and ”Information store for public folders“.

When a private information store (mailbox store) is installed, access is explicitly forbidden for the groups ”Domain admins“, ”Enterprise Admins“ and the administration account itself because of the changes to the Microsoft Exchange Server 2000/2003 security concept. This results in a logon to a user’s mailbox being denied to an administration account in the Active Directory domain. A logon procedure is implicitly executed when mailbox statistic data (number of entries and their size) is determined. If this functionality needs to be restored, you have to ensure that access permissions are set on each mailbox for the Quest One Identity Manager user account.

Setting up the Identity Manager Database for Synchronization with a Microsoft Exchange Environment

Configuration Parameters Setting Up a Microsoft Exchange Environment

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\ADS	Supports the area of Active Directory. This is a preprocessor relevant parameter. The database needs to be recompiled after it has been changed.
TargetSystem\ADS\Exchange2000	Supports the area of Active Directory with Microsoft Exchange. This is a preprocessor relevant parameter. The database needs to be recompiled after it has been changed.
TargetSystem\ADS\Exchange-2000\Exchange2007	Preprocessor relevant configuration parameter for controlling model components for administration of a Windows 2000 target system with Active Directory Service (ADS) and Microsoft Exchange 2007. If set, the database needs to be compiled if changes are made to the parameter.
TargetSystem\ADS\Exchange-2000\Exchange2010	Preprocessor relevant configuration parameter for controlling the database model components for Window 2000/ 2003 target system admin with Active Directory Service (AD) and Exchange 2010. If the parameter is set the Exchange 2010 function extensions are available. Changes to the parameter require recompiling the database.

Prerequisites for reconciling Microsoft Exchange environment with the Identity Manager database are:

- Regular synchronization with the Active Directory environment.
  Refer to section Setting Up Active Directory Synchronization on page 202.

- The configuration parameter ”TargetSystem\ADS\Exchange2000“ is set. Depending on which version of Microsoft Exchange Server is in use, the configuration parameter ”TargetSystem\ADS\Exchange2007“ or ”TargetSystem\ADS\Exchange2010“ is set.
  This shares the database components for this version of the Microsoft Exchange Server. The configuration parameters are preprocessor relevant. The database needs to be recompiled after it has been changed. Read the sections Compiling an Identity Manager Database on page 100 in the Getting Started Manual and section Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual for more information.

- The synchronization server is set up.
  Prerequisites for installation are described in section Installation and Configuration of a Microsoft Exchange Synchronization Server on page 258. Section Declaring the Microsoft Exchange Synchronization Server on page 261 explains how to set up the server in the Identity Manager database.

- The Active Directory domain is extended with Exchange relevant data. For more information see section Active Directory Domain Extended Master Data for Synchronizing with Microsoft Exchange on page 263.

- Synchronization is configured and the sheduled task is started.
  Use synchronization configuration to specify which Microsoft Exchange objects will be synchronized between the target system and the Identity Manager database and in which way. See section Table How to Configure Synchronization with a Microsoft Exchange Environment on page 264 for more information.

Declaring the Microsoft Exchange Synchronization Server

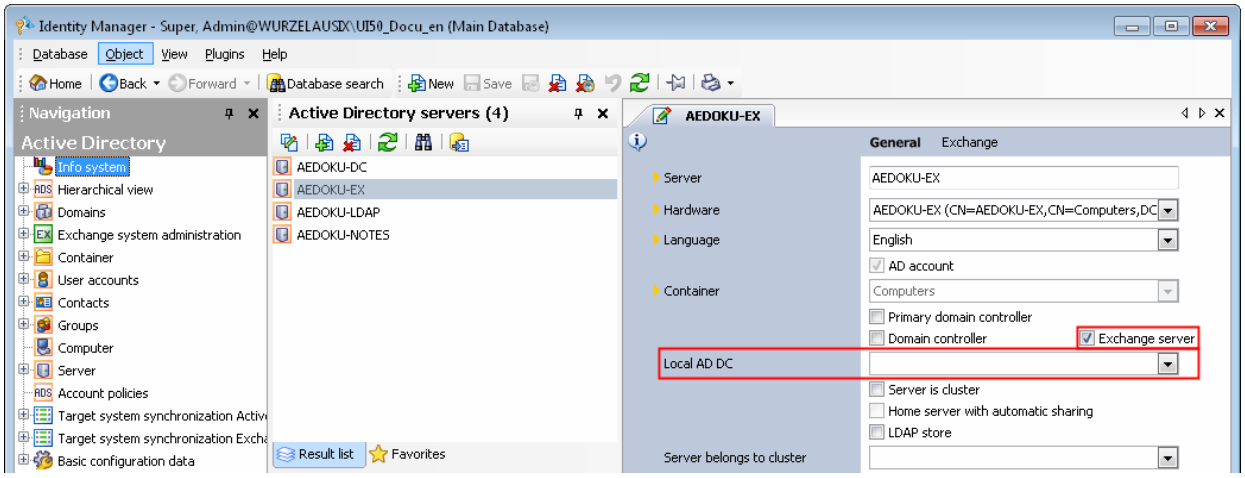
Tools: Identity Manager with application role <target system>/<Active Directory Service>; Manager

A Microsoft Exchange Server is declared in the Identity Manager in the category <Active Directory>. In the filter <Server>, all the Active Directory servers are shown. These have already been made public in the Identity Manager database through synchronization with the Active Directory environment. Select an Active Directory server that Microsoft Exchange Server will be installed on and make the following adjustments on the <General> tab:

- Label as Exchange Server
  This server is used for synchronization of exchange relevant object properties. If the server acts as a domain controller at the same time, access to Active Directory is also executed using this server.

- Optional entry if a local Active Directory domain controller
  You can enter a domain controller that is physically near for a Microsoft Exchange Server on a member server through which Active Directory is accessed. If no server is entered, the central Active Directory domain Active Directory synchronation server is used for process handling.

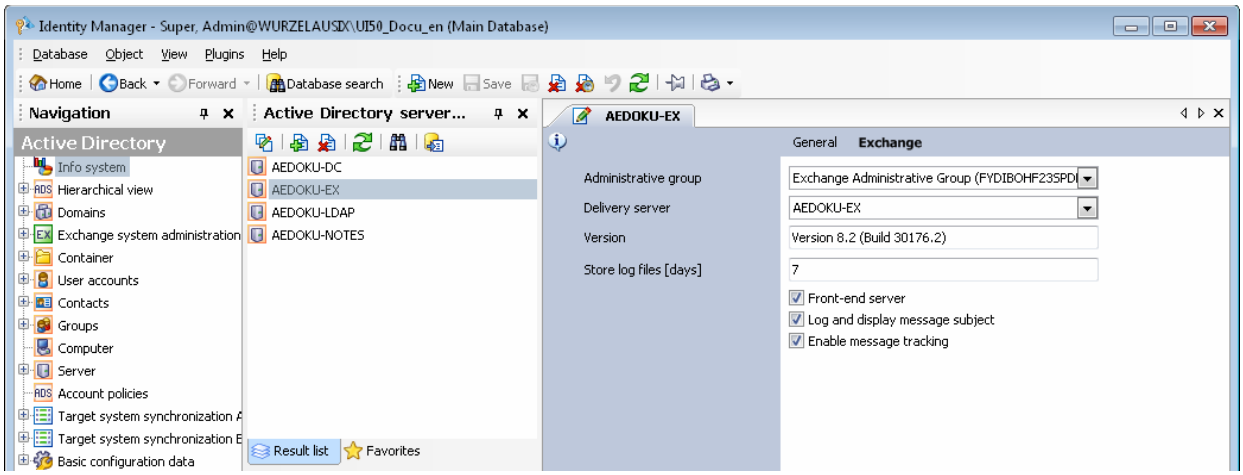
Setting Up a Microsoft Exchange Synchronization Server



This data is however has no meaning for the server as synchronization server and therefore should be not made until after initial synchronization.

Further Exchange relevant input (tab <Exchange>) is determined by synchronization and entered into the database.

Setting Up a Microsoft Exchange Synchronization Server



This data includes:

- Server administration group
- Microsoft Exchange Servers version
- Server for X.400 Services (delivery server)
  This name identifies the Message Transfer Agent (MTA) over the other mail systems. This entry normally matches the name of the server where the X.400 server is installed.
- Label as front end server
- Specifies whether message subject should be logged and displayed.
  Messages can be tracked cross-server with this message status. In order to show the server's message status you need to activate the message subject log.
- Specifies whether massage tracking is active on this server.
- Period of time for storing log files from message tracking on the server.

Determining the Valid Data Synchronization Server

Configuration Parameters for Determining the Exchange Server

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\Exchange2000\UseAlwaysEx2kSyncServer	This configuration parameter specifies the Exchange synchronization server on which the action in the target system should take place.

In order to synchronize data between the Microsoft Exchange environment and the Identity Manager environment you need to ensure access to a Microsoft exchange server on the one hand and Active Directory on the other. The Identity Manager offers various methods to determine the server from the different configurations of Active Directory with Microsoft Exchange.

Microsoft Exchange Server Also Acts as a Active Directory Domain Controller

If a Microsoft Exchange server is also a domain controller, this server is used to access Active Directory relevant object properties as well as Exchange relevant object properties.

The Microsoft Exchange Server is a Active Directory Member Server

If an Microsoft Exchange server is also an Active Directory member server, this server is used to access Active Directory relevant object properties as well as Exchange relevant object properties. The local Active Directory domain controller for accessing Active Directory relevant object properties is determined that is entered in the Identity Manager database for this Exchange server. If there is not local Active Directory domain controller, the central Active Directory synchronization server for the Active Directory domain is used to handle Active Directory relevant processes.

There is an Exchange Server in the Identity Manager Database

The Microsoft Exchange Server is declared in the Identity Manager database as the Exchange server and entered in the Active Directory domain as exchange synchronization server. Thie server is used for scheduled synchronization and for single processing tasks like creating or modifiying Microsoft Exchange objects.

There are Several Exchange Server in the Identity Manager Database

The Microsoft Exchange Servers are declared in the Identity Manager database as Exchange servers. The Exchange server for scheduled synchronization is entered as Exchange synchronization server in the Active Directory domain.

The Exchange server for executing single processing tasks is selected via the configuration parameter TargetSystem\ADS\Exchange2000\UseAlwaysEx2kSyncServer. If the configuration parameter is set, the Exchange synchronization server for the Active Directory domain is used for all exchange relevant actions. If the parameter is not set, the Exchange server is determined from the user's mailbox store.

Overlapping Server Selection for Scheduled Synchronization

Only one fixed Exchange synchronization server can be entered in the Identity Manager database for an Active Directory domain. One other synchronization server can be entered in the synchronization configuration in order to react quickly to other demands. This server is used rather than the fixed Exchange synchronization server but only for synchronizing with this synchronization congfiguration. The server does not necessarily have to be known to the Identity Manager database.

Active Directory Domain Extended Master Data for Synchronizing with Microsoft Exchange

Tool: Identity Manager with application role <target system>/<Active Directory Service>; Manager

Read section Setting Up an Active Directory Domain on page 206 to find out how to declare an Active Directory domain in an Identity Manager database. The domain master data that is relevant for synchronizing the Identity Manager database with a Microsoft environment is explained here. This includes:

- Exchange synchronisation server
  If there are several servers available for synchronizing with Microsoft Exchange system, the server to be used to run process each task is determined dynamically. In large systems, this behavior can, in certain circumstances, cause Microsoft Exchange objects to be processed on a server in a branch office and even with a time delay. Enter a fixed synchronization server here, in order to prevent this behavior. This server will then be used for handling Microsoft Exchange objects. For more information read section Determining the Valid Data Synchroni-

zation Server on page 262.

Please note the following:
Only those servers that manage their own Active Directory container in the Active Directory domain are shown in Identity Manager. This means that, in certain circumstances, it might be necessary to enter the synchronization server using the Manager.

- Exchange version in use
  Microsoft Exchange Server Versions 2000, 2003, 2003 service pack 2, 2007 and 2010 are supported.

- Exchange mapping file
  The mapping file contains the templates for mapping target system specific objects, such as user accounts, groups or hardware objects, between the Identity Manager database and Windows NT domains. The evaluation is executed using target system specific process components. An external mapping file only has to be given if the default mapping for the data should not be used. This external mapping file must exist on the synchronization server. If no path is given, the mapping file has to be in the Identity Manager Service install directory on the synchronization server. Refer to the section Customizing Mapping rules on page 180 or further infomation.

- Exchange account resource
  This data is required when Microsoft Exchange mailboxes in this Active Directory domain should be managed through a user account resource. Read more in section Administration of Microsoft Exchange Mailboxes via User Account Resources on page 284.

How to Configure Synchronization with a Microsoft Exchange Environment

Tool: Manager

The basic principles of data synchronization can be found in the chapter Data Synchronization in Identity Manager on page 161. The follow steps are required to configure synchronization between the Identity Manager database and a Microsoft Exchange environment:

- Customize configuration parameters relevent for synchronization
  See section Configuration Parameters for Synchronizing with Microsoft Exchange on page 264 for more information.

- Set up the synchronization configuration
  The basic procedure for this is described in the section How to Configure Synchronization on page 163. Special setting for synchronizing with an Active Directory domain are explained in section Special Features of Microsoft Exchange Synchronization Configuration on page 265.

- Configuring mapping rules
  The basic procedure for this is described in section How to Define a Mapping on page 175.

You can find detailed information about analyzing the synchronization and handling synchronization errors in section Synchronization Analysis on page 176.

Configuration Parameters for Synchronizing with Microsoft Exchange

The following only list the configuration parameters that are relevant for scheduled synchronization. Other configuration parameters can be effective for target system relevant actions, for example, insert, change or deletion of users in the database and their prompt transfer in the target system via the Identity Manager Service.

You can find the full list of configuration parameters in the Designer. The configuration parameters are edited in the Designer. See chapter System Configuration Parameters on page 214 in the Configuration Manual.

Some configuration parameter are preprocessor configuration parameters. This means the database has to be compiled after this parameter is changed. For more information see section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and section Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual.

Configuration Parameters for Synchronizing with a Microsoft Exchange Environment

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\Exchange2000\DefaultAddress	This configuration parameter contains the default email address for messages when actions in the target system fail.
TargetSystem\ADS\Exchange2000\MaxFullsyncDuration	Specifies the maximum runtime for synchronization. During this time, no new group membership calculations are made via the DBScheduler.
TargetSystem\ADS\Exchange2000\RedoDelay	This configuration parameter specifies the delay time after which an incompleted update is repeated. The input is in minutes.
TargetSystem\ADS\Exchange2000\SingleThread	Specifies whether synchronization objects should be saved synchronously. The objects are saved asychronously by default. If the parameter is set, saving is synchronous, which increases the synchonization runtime.

Special Features of Microsoft Exchange Synchronization Configuration

Read section How to Configure Synchronization on page 163 about basic synchronization configuration. At this point, we are only going to look at the special features relevant to the synchronization configuration for Microsoft Exchange. The following synchronization configuration tasks are available for an Active Directory domain.

Configuring Synchronization

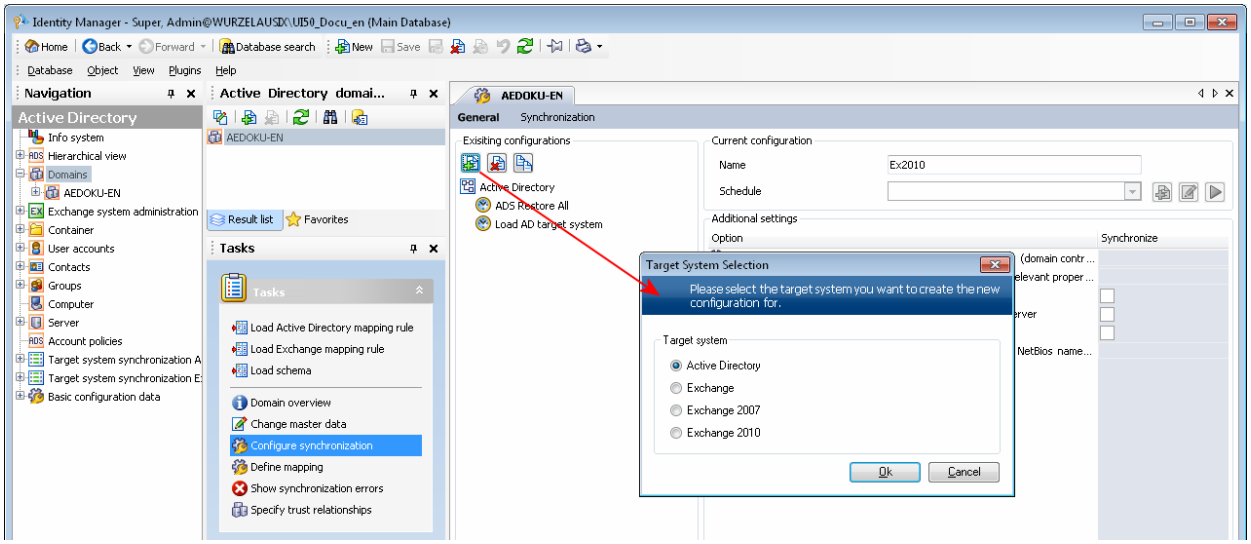
Use this form to set up the synchronization configuration. Enter the basic synchronization configuration and the schedule on the <General> tab. If necessary, you can manually start synchronization from here. On the <Synchronization> tab, specify how objects should be handled during synchronization.

For a new synchronization configuration first select the target system ”Exchange“ or ”Exchange 2010“. These are available:

- ”Active Directory“ for synchronizing with an Active Directory domain
- ”Exchange“ for synchronizing with a Microsoft Exchange Server 2000, Microsoft Exchange Server2003 or Microsoft Exchange Server 2007
- ”Exchange 2010“ for synchronizing with a Microsoft Exchange Server 2010

The configuration is carried out as described in section How to Configure Synchronization on page 163.

Selecting the Target System in the Synchronization Configuration



The following options are available on the <Additional settings> pane on the <General> tab:

- Synchronization server for comparing with Active Directory (domain controller)
  If the Exchange synchronization server is not an ACtive Directory domain controller then enter a server here that can access Active Directory relevant object properites. This input is only required if the Active Directory domain synchronization server is not used (see Determining the Valid Data Synchronization Server on page 262).

- Synchronization server for comparing the Exchange 2000 relevant properties
  Here you enter the Microsoft Exchange server for synchronizing Exchange relevant object properties. This input is only required when if the Active Directory domain synchronization server is not used (see Determining the Valid Data Synchronization Server on page 262).

- Determine mailbox size and number of saved objects

- Only synchronize mailboxes located on the synchronization server
  This option specifies whether a server's mailboxes or the entire Microsoft Exchange mailboxes should be synchronized. If this option is set, all distribution groups and all mail forwarding addresses for the whole directory are included in the synchronization, however, only those mailboxes that are in the local mailbox store for the synchronization server.

- Exclude mail fowarding addresses from synchronization

- Also look for group members in following domains (delimit NetBios names with a comma)
  The group memberships for Active Directory user accounts are determined in these domains during synchronization. This includes domains in a domain tree or trusted domains.

Defining a Mapping

Use this task to specify how the structure of properties belonging to the object types to be synchronized is mapped in the database and in the target system. The configuration of assignments is described in detail in section How to Define a Mapping on page 175.

Displaying Synchronization Errors

This task provides an alternative method for analysing the synchronization in addition to the Identity Manager Service log file. The objects and dependencies which failed during synchronization are shown

on the form. A detailed description of the error is displayed. The section Logging Synchronization Errors on page 176 provides more detailed information.

Microsoft Exchange Structure

The structure elements in Microsoft Exchange that are not server dependent, are matched by each Microsoft Exchange Server. This effects the organization, administrative groups, global address lists, offline address lists and the folders. Double entries are avoided by running a check routine immediately before entry in the Identity Manager database.

Microsoft Exchange structure objects below server level are only matched by the respective server itself. This effects storage groups, mailboxes and the information store for public folders.

The names and frequency of the structure objects listed below can vary depending on the version of the Microsoft Exchange server in use.

Graphical Representation of the Microsoft Exchange Structure in the Identity Manager

Tools: Identity Manager mit application role <target system>/<Active Directory Service>; Manager

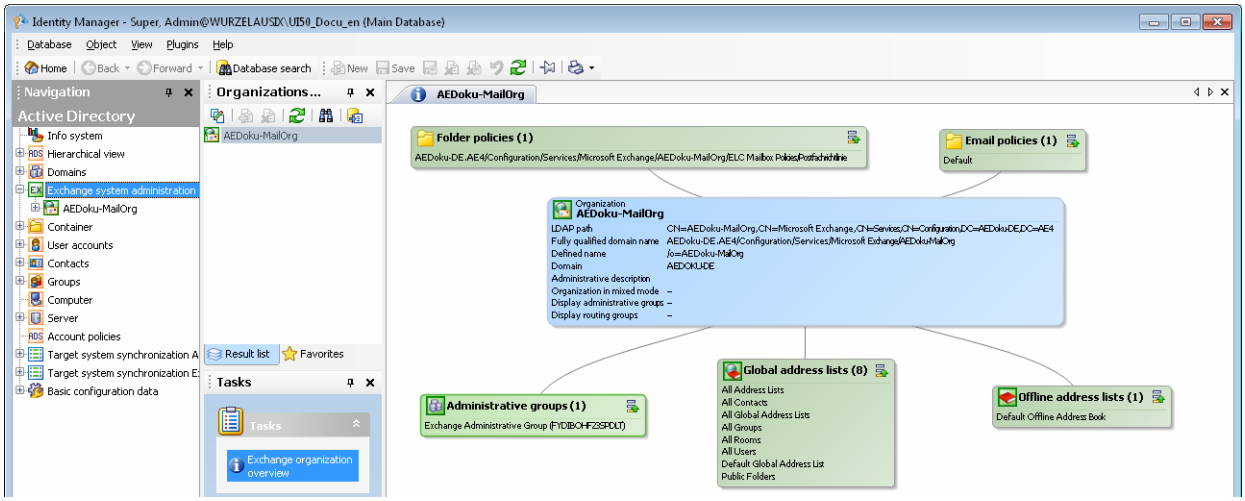
The system information for the Microsoft Exchange structure is loaded into the Identity Manager database during data synchronization. It is not possible to customize this system information due to the complex dependencies and far reaching effects of changes.

The graphical representation of the Microsoft Exchange structure is seen in the category <ActiveDirectory Service>\<Exchange system administration>.

Microsoft Exchange Organization

The Microsoft Exchange organization is defined during the installation if the Microsoft Exchange Server and cannot be modified later. Global settings, address lists and administrative groups are displayed under an Exchange organization.

Displaying Microsoft Exchange Organization



The following properties are displayed:

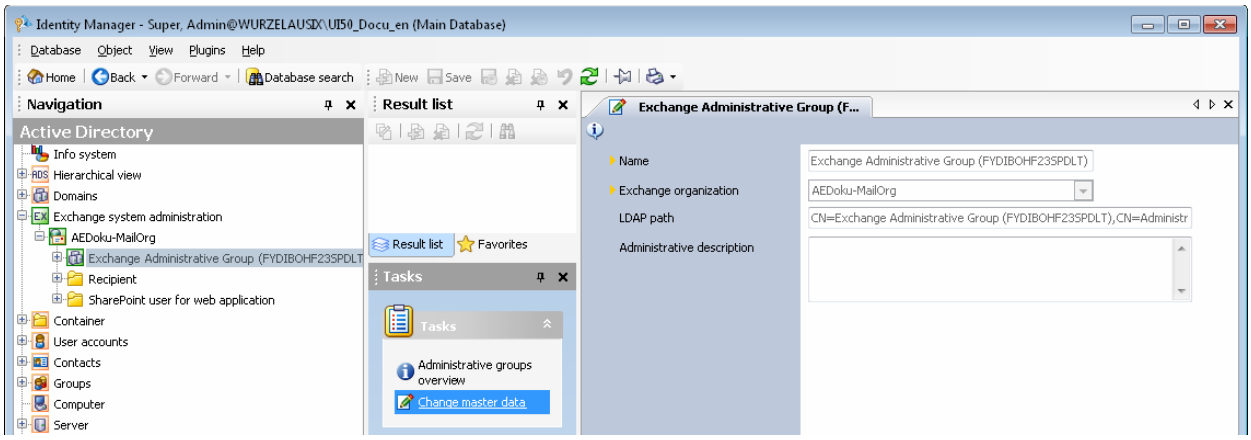
- Name of the organization
- LDAP path to organization
- Fully qualified domain name and distinguished name
- Active Directory domain name
- An administrative description about the organization
- Option whether the organization works in mixed or single mode
- Option to show the administrative groups and routing groups

The global settings for message delivery are not made in the Identity Manager.

Microsoft Exchange Administrative Groups

Administrative groups are used to structure the organization logically. Servers can be collected into managable units within administrative groups. In addition, folder structures can be stored in administrative groups. An administrative group that always exists is the ”First“ administrative group.

Displaying an Administrative Group



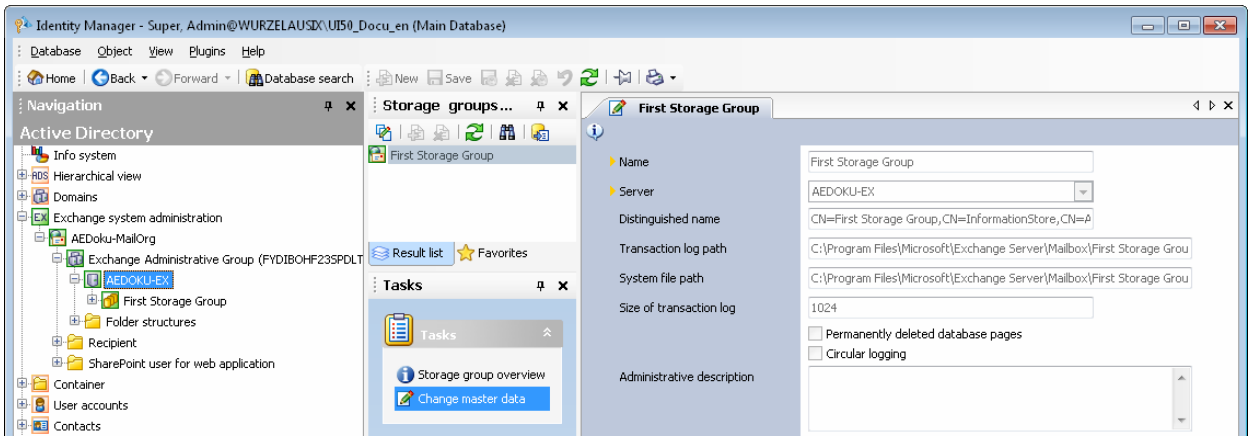
The following properties are displayed:

- The name of the administrative group
- The Microsoft Exchange organization
- LDAP path to administrative groups
- Administrative description of the administrative goup

Microsoft Exchange Storage Groups

Microsoft Exchange Server manages information stores in logical groups. A storage group contains mailbox stores and information storage for public folders as well as the associated transaction log files.

Setting Up a Storage Group



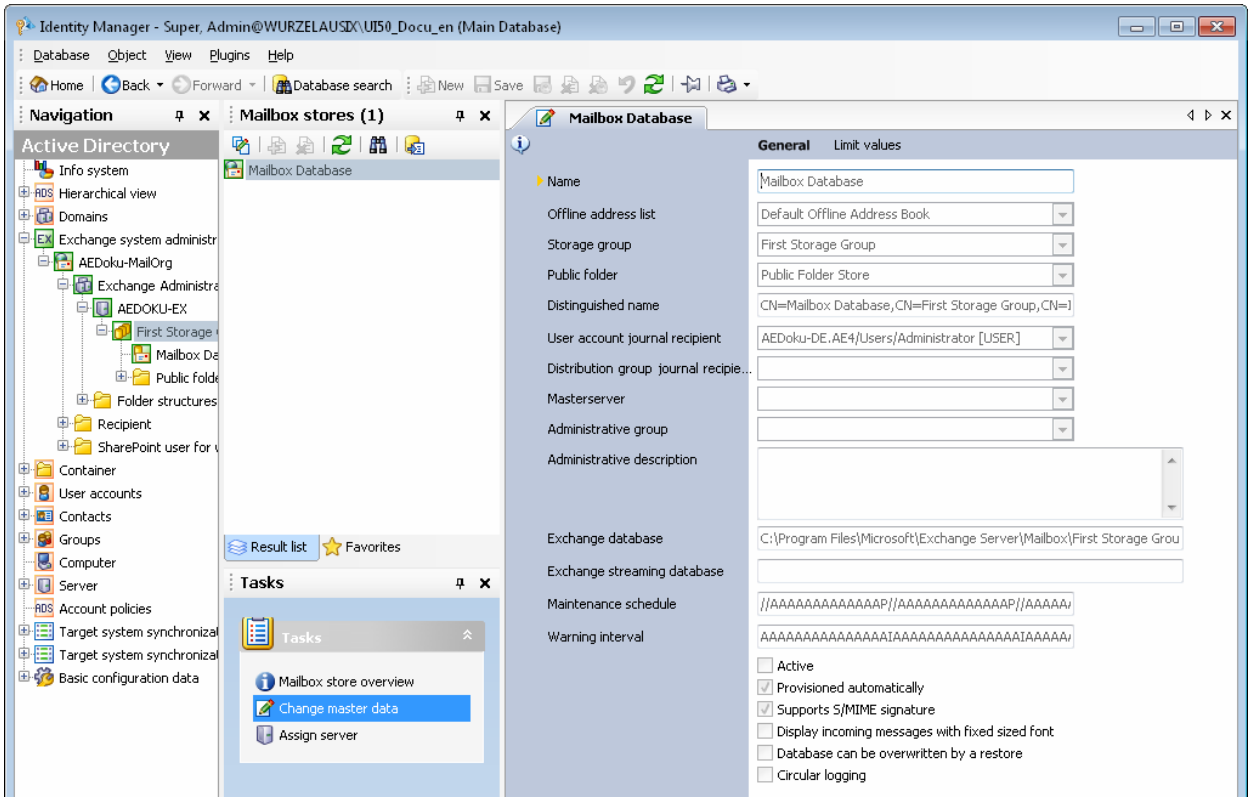
The following properties are displayed:

- Name of the Storage group
- Microsoft Exchange Server
  This server is used to create mailboxes. The server's administrative group is determined internally from the data from this server.
- Distinguished name
  The distinguished name is made up of the store and the adminstration group from the Microsoft Exchange Server.
- Database path
  Enter the paths for storing the transaction logs and the system files. These are valid for all storage group information stores.
- Transaction log size
- Labels deleted database pages to be permanently deleted.
- Circular logging data
  If this option is set, log files are reused and not created new.
- Administrative description for the store

Microsoft Exchange Mailbox Store

A mailbox store is the part of the information store where user mailbox data is kept. Each mailbox store is connected to a public store and a standard offline address list.

Setting Up a Mailbox Store



The following properties are displayed:

- Name of the mailbox store
- Default offline address list
- Store
- Information store for public objects
- Distinguished name
  The distinguished name is made up of the mailbox store name and the store group.
- Mailbox store journal recipient
  A mailbox or a distribution group can be entered here. All messages sent via the mailbox store are logged in this mailbox/distribution group.
- Master server (from Microsoft Exchange Server 2010 onwards)
  If the mailbox store is a copy then here you enter the server where the orginal is stored.
- Path to the Exchange database and the Exchange Streaming database
- Maintenance schedule data (from Microsoft Exchange Server 2007 onwards)
- Warning message interval (from Microsoft Exchange Server 2007 onwards)

- Providing mailbox store status
  The option <Provided automatically> specifies whether the mailbox store is automatically provided or not. The actual status of the mailbox store is shown by the <Active> option. Mailbox store mailboxes can only be used when the memory is available.

- S/MIME signature support
  This option is set when clients that use this mailbox store support S/MIME (Secure Multipurpose Internet Mail Extension).

- Label incoming messages to have fixed font size.

- Specify if the database should be overwritten on restore

- Circular logging data (from Microsoft Exchange Server 2010 onwards)
  If this option is set, log file are reused and not created new.

- Memory limits
  When these limits are reached a warning is gernerated (warn from [KB]) that sending (Prohit send from [KB]) as well as sending and receiving messages (prohibit transfer from [KB]) is prohibited.

- Storage time for deleted objects and mailboxes
  The option <Do not delete permanently before making a backup> permits deletion of objects only after a backup has been made.

Microsoft Exchange Public Folder

Information stores for public folders are linked to a public folder structure.

Enter the following properties are displayed:

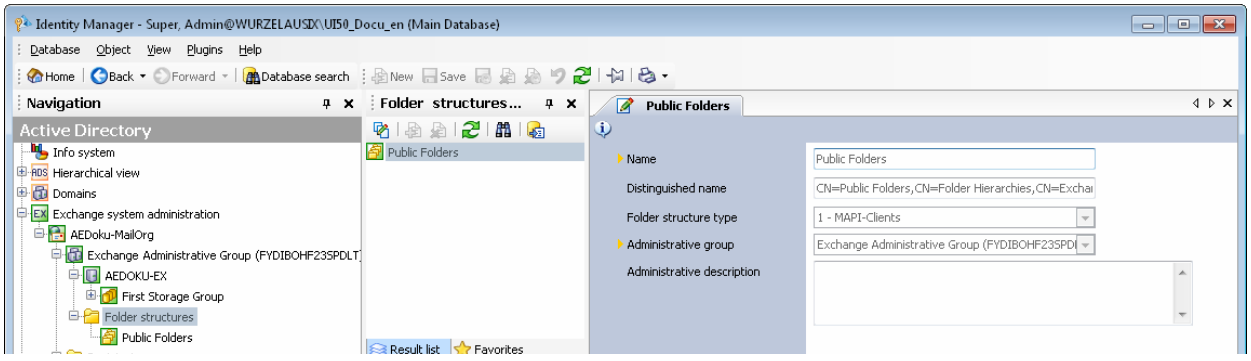
- Name of the folder structure

- Administrative group

- Folder structure type
  This regulates which function the folder has and as a result, who has access and with which protocol (general purpose (IMAP4 protocol), MAPI clients (public mail folder; MAPI logins and IMAP4 protocol), NNTP clients (News folder; NNTP protocol). Folder structure types are displayed in the category <Basic configuration data><Folder structures>.

- Administrative description

Folder Structure

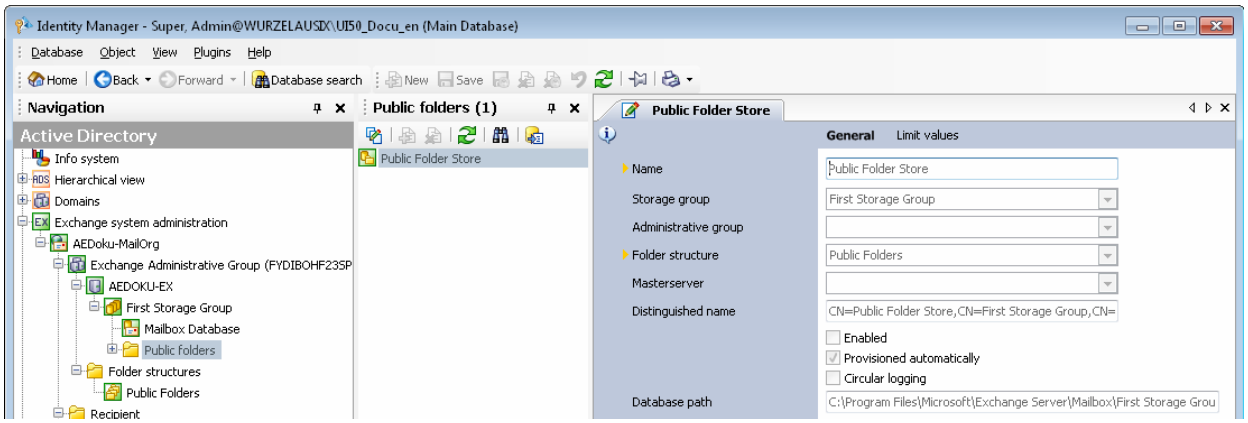


The following properties are displayed:

- Public folder name a
- Store group
- Administrative group
- The associated folder structure
- Master server (from Microsoft Exchange Server 2010 onwards)
  If the mailbox store is a copy then here you enter the server where the orginal is stored.
- Email address and email alias
- Master server (ab Microsoft Exchange Server 2010)
  If the public folder is a copy, enter the server here where the original copy can be found.
- Distinguished name
  The distinguished name is made up of the mailbox store name and the store group.
- Providing mailbox store status
  With the option <Provided automatically>, you specify whether the folder is automatically provided or not. The actual status of the folder is shown by the <Active> option. Folders can only be used when the memory is available.
- Circular logging data (from Microsoft Exchange Server 2010 onwards)
  If this option is set, log file are reused and not created new.
- Path to the Exchange database and the Exchange Streaming database
- Administrative description
- Memory limits for public folders
  When these limits are reached a warning is gernerated (warn from [KB]) that sending (Prohit send fpom [KB]) as well as sending and receiving messages (prohibit transfer from [KB]) is prohibited.
- Expiry data for the folder in this information store in days
- Replication setting for public folders
  When replication is continually executed a <Replication interval> is given in minutes. A maximum size is defined for replication messages (Max. sending size [KB]).

- Storage time for deleted objects
  The option <Do not delete permanently before making a backup> permits deletion of objects only after a backup has been made.

Setting Up Information Storage for a Public Folder



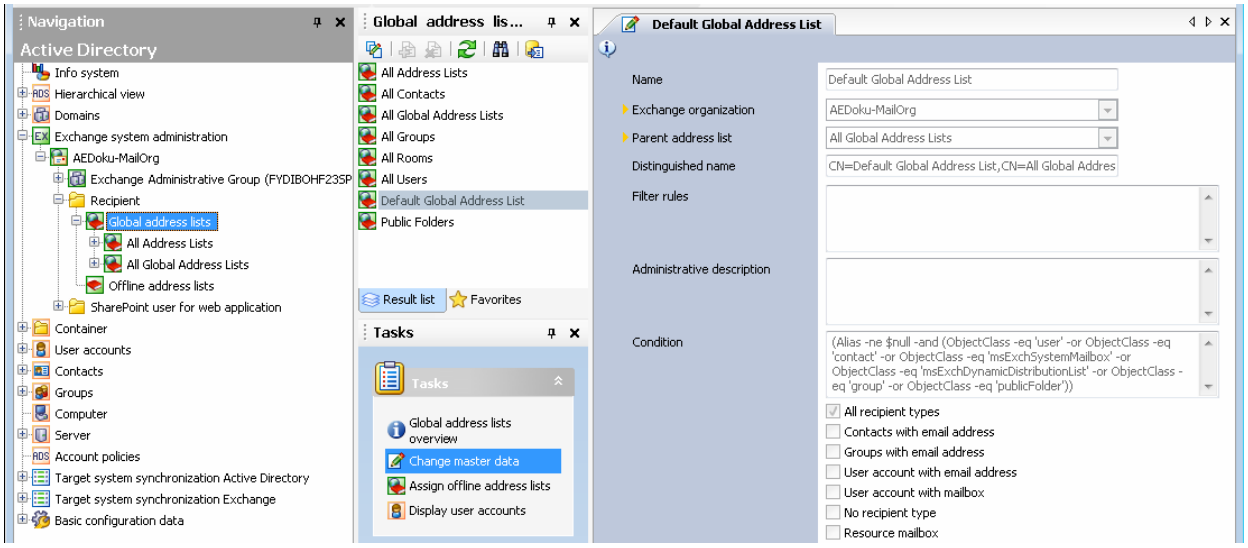
Microsoft Exchange Address Lists

Configuration Parameters for Microsoft Exchange Address lists

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\Exchange2000\ DefaultGlobalAddressList	A least one global address list needs to be included when an off-line address list is added in Microsoft Exchange. This is normally the default global address list. If the parameter is not set the first global address list found is assigned as member.

Microsoft Exchange offers you the possibility to manage address lists for your Microsoft Exchange organization. Members in address lists can be users, email activated users, contacts or groups and public folders. Address lists are shown in Identity Manager in the category <Active Directory>\<Exchange system administration>\<Exchange organization>\<Recipient>.

Displaying a Global Address List



The following properties are displayed:

- Name of the global address list
- Microsoft Exchange organization
- Parent address list
- Distinguished name
  The distinguished name is made up of the address list, the parent address list, the contained and the Microsoft Exchange organization.
- Filter rules for defining members
- Assigned users and offline address lists
- Addtional conditions for the filter rules (from Microsoft Exchange Server 2007 onwards)
- Administrative description for the global address list
- Angaben, welche Empfängertypen zulässig sind (ab Microsoft Exchange Server 2007)
- Assigned users and offline address lists (tasks <Assign offline address lists>) and <Display user accounts>.

Offline address lists allow a mailbox user to get the address list data and work with it offline. The following properties are displayed:

- Name of the offline address list
- Microsoft Exchange organisation
- Parent offline address list
- Distinguished name
  The distinguished name is made up of the offline address list name, the parent offline address list, the container and the Microsoft Exchange organization.
- Microsoft Exchange Server where the offline address list is stored.
- Administrative description of the offline address list
- Data supporting Outlook versions (from Microsoft Exchange 2007)
- Default offline addresslist label (from Microsoft Exchange 2007)
- Update interval for offline address lists
- Assigned global address list (task <Assign global address lists>

Policies for Mobile Email Queries

Mailboy policies for mobile email queries contain setting that come into effect when data is accessed in the Microsoft Exchange organization with mobile devices via Microsoft Exchange synchronizations protocol Exchange ActiveSync. The settings include, for example, password requirements, specifications for email attachments, device encryption data and access rules for shares. These mailbox policies are in place as from Microsoft Exchange server 2007 upwards.

Mailbox policies for mobile email queries are displayed in the category <Active Directory>\<Exchange system administration>\<Exchange organization>\<Policies>\<Email policies>. The following properties are displayed:

- Policy name
- Distinguished name and full name for the policy
- Attachments download permitted
  If the option is enabled. attachments are automatically downloaded.
- Maximum size of mail attachment
  Gives the maximum size of the attachments that are automatically downloaded.
- Device permitted without full policy
  The setting specify whether older devices can connect to the Exchange server via Exchange ActiveSync.
- Lock when inactive
  This setting specifies how many minutes should pass without activity vefore the device is locked.
- Password required
  If this option is set, a password is required for the device.
- Simple password
  This option specficies whether a simple password is sufficient.
- Alphanumeric characters required
  This option specifies whether alphanumeric characters are expected in the password.
- Minimum length of password
  This option specifies the minimum number of characters that the password must have.
- Password validity period
  This option speifies the length of time that a password can be used for before a new one is required.
- Password cycle
  This option specifies the number of new password that a user has to use before an „old" one can be reused.
- Password restorable
  This option specifes whether a retore password is generated that can be used to unlock the device.
- Maximum number of error messages
  This option specifies the numer of invalid password that can be entered. If the user has reached the limit the user account is blocked.
- Encrypt password
  This setting specifies whether device encryption is required.
- File share
  This option specifies whether file sharing is permitted.
- SharePoint services
  This option specifies whether access to Microsoft SharePoint Service files is permitted.

- Assigned Active Directory user accounts
  Use the task <Assign user> to assign the mailbox policy to Active Directory user accounts.

Folder Administration Policies

From Microsoft Exchange Server 2007 onwards, mailbox policies are used to group together administrated folders. Administration folders are made available when a policy is assigned to an Exchange Organization user.

Mailbox polices for folder administration are displayed in the category <Active Directory>\<Exchange system administration>\<Exchange organization>\<Policies>\<Folder policies>. The following properties are displayed:

- Policy name
- Distinguished name and full policy name
- Assigned Active Directory user account
  Use the task <Assign user account> to assign the mailbox policy to Active Directory user accounts.

Policies for Shares

From Microsoft Exchange Server 2010 onwards, policies for shares are implement to make calendar and contact data available. Assigning a share policy to a user account regulates how calendar and contact data can be shared with user accounts outside the Exchange organization.

Share policies are displayed in Identity Manager in the category <Active Directory>\<Exchange system administration>\<Exchange organization>\<Policies>\<Share policies>. The following properties are displayed:

- Policy name
- Distinguished name and full name of policy
- Shared domain
  Contains the domains and actions valid for this share policy.
- Specifies whether this policy is enabled
  The calendar and contact data is shared for the user account of the given domains.
- Assigned Active Directory user account
  Use the task <Assign user account> to assign the share policy to Active Directory user accounts.

Microsoft Exchange Recipients

Microsoft Exchange distinguishes between email and mailbox enabled recipients. Recipients can be users, contacts and groups. Mail-enabled recipients can simply receive messages, mailbox-enabled recipients can send, receive and save messages. There is at least one email address defined for an email recipient. A mailbox-enabled user is always connected to a Exchange mailbox. Active Directory user accounts in Microsoft Exchange can either be mailbox-enabled recipients or mail-enabled recipients. Contacts and groups on the other hand, can only be mail-enabled recipients. For further explanation of the concepts, read the documentation for your Microsoft Exchange Server.

The key aspects of administrating a Microsoft Exchange environment with the Identity Manager are represented by:

- Mailboxes
- Email users and email contacts
- Distribution groups

Setting Up Microsoft Exchange Mailboxes

Tools: Identity Manager with application role <Target system>/<Active Directory>; Manager

Define Microsoft Exchange mailboxes for Active Directory user accounts in the category <Active Directory Service>\<User accounts>. The names and frequency of the master data and tasks listed below can vary depending on the version of the Microsoft Exchange server and the mailbox type of the Microsoft Exchange mailbox.

It is recommended to use user account resources to set up mailboxes for company employees. Some of the following data is created using templates if a user account resource is used for configuring the mailbox. The extent of inheritance depends on the manage level of the Active Directory user account. The templates that are supplied can be customized.

Supported Mailbox types as from Microsoft Exchange Server 2007

As from Microsoft Exchange Server 2007 the following mailbox types are supported:

- User mailbox
  Use mailboxes are assigned to Active Directory user accounts in an Exchange organization.
- Equipment and room mailbox
  These mailboxes are resource mailboxes that are used for planning resources. Properties for booking and planning resources are support as from Microsoft Exchange Server 2010 in the Identity Manager.
- Legacy mailbox
  Legacy mailboxes are mailboxes that are kept in a mixed Microsoft Exchange environment on a Microsoft Exchange 2000/2003 Server. These mailboxes are loaded in the Identity Manager by sychronization and cannot be edited.
- Linked mailbox
  Linked mailboxes are assigned to users in a trusted domain. This makes the Exchange organization available within a domain. Users in a trusted domain without an Exchange structure can obtain a linked mailbox in this Exchnage organization.
- Shared mailbox
  Shared mailboxes are mailboxes that are used by several users.

Enabling a Microsoft Exchange Mailbox

Select the Active Directory user account and run the task <Activate Exchange extensions>. This makes the input data for Microsoft Exchange mailbox visible and it can be edited. The mailbox is created when the changes are saved.

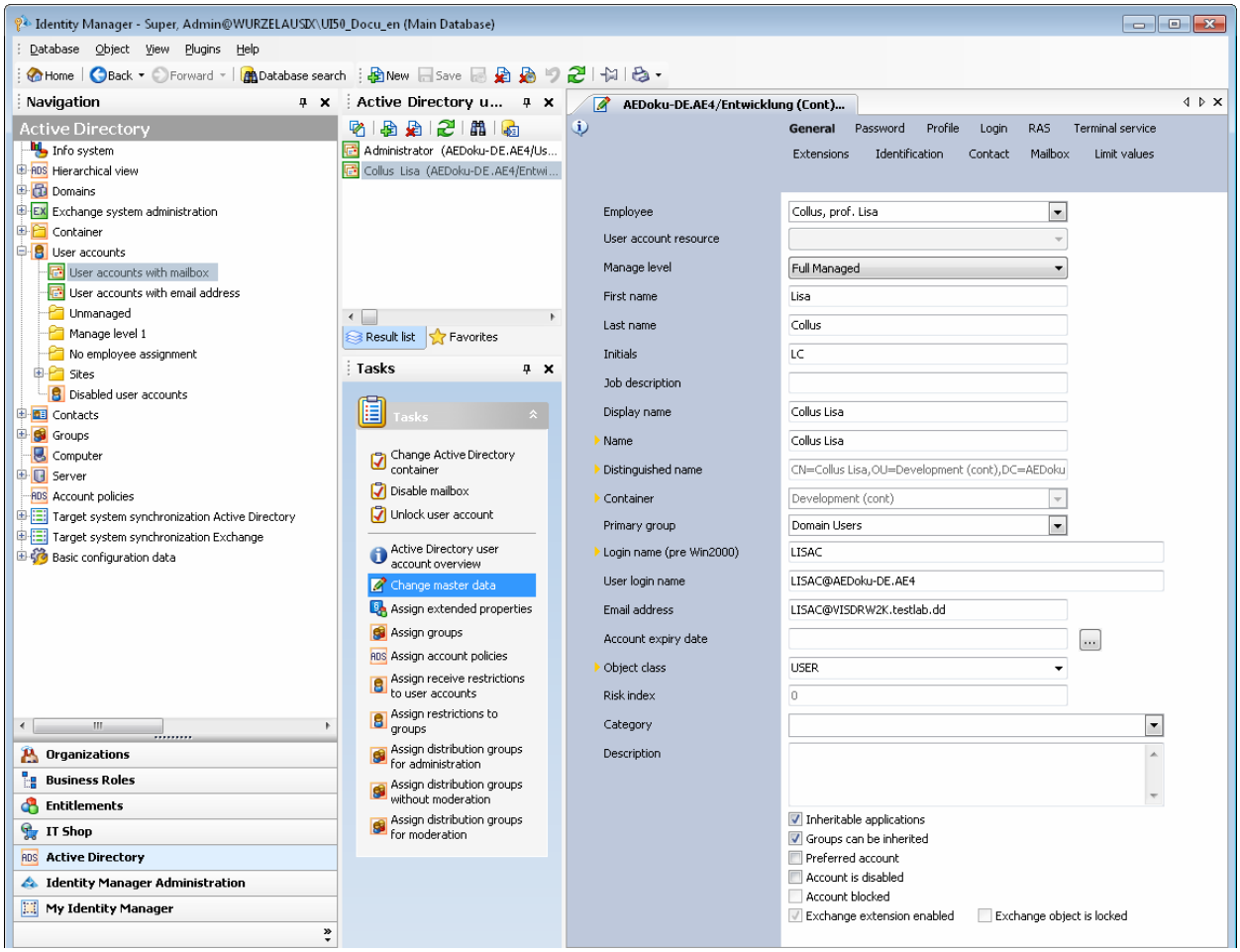
Please note that a user can either be mailbox-enabled or mail-enabled. If a user is already mail-enabled, you have to disable the user with the task <Disable email address> and then you can set up a mailbox. To disable the mailbox at a later date, run the task <Disable mailbox>.

Active Directory user accounts that own an Exchange extension are labeled with the option <Exchange extension enabled>. If the Exchange extension is disabled the option <Exchange object is locked> if set.

Microsoft Exchange Mailbox Master Data

Enter the master data for the Microsoft Exchange mailbox on the tab <Mailbox>.

General Data for a Microsoft Exchange Mailbox



The minimal requirements for enabling a Microsoft Exchange mailbox are:

- Selecting the mailbox type (Microsoft Exchange Server 2007 or later)
  The mailbox type is specified when the mailbox is added and cannot be changed later. You can select one of the following mailbox types: user mailbox, room mailbox, equipment mailbox, linked mailbox, legacy mailbox or shared mailbox. Refer to section Supported Mailbox types as from Microsoft Exchange Server 2007 for more information.

- Mailbox store data
  The mailbox store is part of the information store. The mailbox data (received messages, attatchments, folders, documents) is saved in the mail on the Microsoft Exchange server. The mailbox store for user mailboxes is determined from the company IT data for the assigned employee depending on the manage level of the user account

- Naming the alias
  The alias should be unique and is used for further identification of the mailbox.

Other properties are:

- Simple display name
  The simple display name is used for systems that cannot interpret all the characters in the normal display name.

- Alternative recipient
  You can either enter an alternative recipient or a recipient group for forwarding the messages to from this mailbox. If the option <Deliver and forward> is set, messages are sent to alternative recipients and the mailbox owner.

- Maximum number of recipients
  You can limit the number of recipients that the mailbox user can send messages to. If there is no limit, the global setting for Exchange organization message delivery in the Exchange system manager.

- Mailbox addressing
  Enter email addresses in X400 format for addressing the mailbox. Set the option <Decrease priority of X400 messages with high priority> when messages with high prority for X400 addresses should be down graded. In the input list <Proxy addresses> you can add further email addresses to the mailbox. You can also use other mail connectors (e.g. CCMail, MS) as address types for default addressing (SMTP, X400). The following syntax should be observed for setting up other proxy addresses:

  ```
  Adress type: new email address
  ```

- Automatic updated based on recipient policies
  If changes that are made to a recipients email address based on the recipient policy need be automatically updated, set the corresponding option.

- Show in address book
  Set the option <Do not display in address list> on the mailbox if you want to prevent the mailbox being displayed in address lists. This option is valid for all address books.

- Protocol settings
  The protocol setting for the permitted connection protocols (Outlook Web Access, IMAP4, POP3, MAPI) for mail clients with this mailbox, are loaded during synchronization and cannot be edited. It is possible to active or deactivate the protocol.

- Mobile access
  You can activate the settings ”Outlook Mobile Access“, ”User Initiated Synchonization“ and ”Up-To-Date Notification“ to configure access via mobile devices under Microsoft Exchange Server 2003.

- Online list information
  Enter the ILS server and the ILS user account for online list information.

- Assistant
  An assistant can be named in the input field <assistant name> or <Assistant>. The assistant is is displayed in the email recipient’s properties in Microsoft Outlook. The entry of an assis-

tant name can be with any text. The name is mapped to the attribute ”msExchAssistant-Name“ in Active Directory. As from Microsoft Exchange Server 2003 the assistant is determined by its Distinguished name and is mapped to the ”Secretary“ attribute in Active Directory.

- User mailbox policies
  Select the mailbox policy for mobile email requests under <Email policies> and the mailbox policy for folder administration unter <Folder policy>. For more information see sections Policies for Mobile Email Queries and Folder Administration Policies.

- Share policies
  Select the share policy valid for this user. Read section Policies for Shares for more about this.

- Linked mailbox
  Linked mailboxes are assigned to users in a trusted domain. This makes the Exchange organization available within a domain. Users in a trusted domain without an Exchange structure can obtain a linked mailbox in this Exchange organization.
  A linked mailbox is only allows for mailboxes with the mailbox type ”linked mailbox“. The external user that has access to the Exchange organization through this mailbox is entered here. The linked mailbox itself is disabled. The Identity Manager Service is responsible for disabling it in Active Directory; after the next syncnronization the linked mailbox is also disabled in the Identity Manager database.

- Archiving data (Microsoft Exchange Server 2010 or later)
  Set the option <Archving enabled> and enter the name of the archive in the input field, <Name of achive>.

- Automatic calendar maintenance (Microsoft Exchange Server 2010 or later)
  Set this option to automatically update changes to meeting data, like time or response in the participants calendar.

- Delete forwarded meetings (Microsoft Exchange Server 2010 or later)
  Set this option to automatically delete messages to other participants about forwarded meetings. These are moved to the ”Deleted objects“ folder.

- Delete expired meeting requests (Microsoft Exchange Server 2010 or later)
  Set this option to automatically delete old meeting requests from the calendar.

- Mark new meeting requests with the status "Tentative" (Microsoft Exchange Server 2010 or later)
  Set this option to automatically enter new meeting requests with the status ”tentative“ in the calendar.

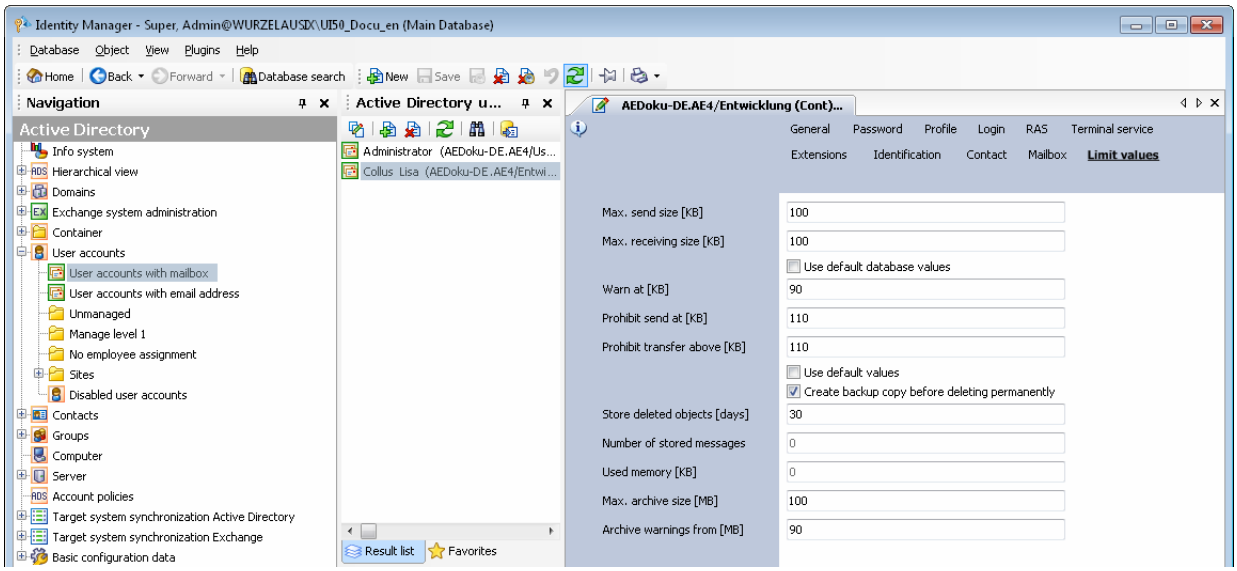
- Permit meeting requests from external senders (Microsoft Exchange Server 2010 or later)
  Set this option if meeting requests from external senders should be entered in the calendar.

- Enable retention hold (Microsoft Exchange Server 2007 or later)
  Set this option if the policies for retention hold should be temporarily suspended, for example for vacation periods. You specify the time period with the <Start date> and <End date>.

Limits for a Microsoft Exchange Mailbox

Enter the limits for a Microsoft Exchange mailbox on the <Limits> tab.

Limits of a Microsoft Exchange Mailbox



- Maximum send size [KB] and maximum receive size [KB]
  Specify the maximum size (in KB) for messages that the user may send or receive. The Exchange organization global settings in the Exchange Manager come into effect for message delivery if there are no limitations. Memory limits for mailboxes are displayed in the same way. When these limits are reached a warning is gernerated (warn from [KB]) that sending (Prohit send from [KB]) as well as sending and receiving messages (prohibit transfer from [KB]) is prohibited. The enabled option <Use default database values> uses the information store limits.

- Do not delete irrevocably before a backup is made
  With this option, you specify if the object is allowed to be deleted after a final backup is run. If the option <Use default values> is activated the values in the information store are valid.

- Store deleted objects [days]
  Specify the maximum retention time for deleted objects in days.

- Number of saved messages and used disk space [KB]
  This data is determined through sychronization and cannot be edited manually. In order to find the value by synchronizing you need to set the configuration option ”Find mailbox sizes and number of stored objects“ in the synchronization configuration. For more information, read section Special Features of Microsoft Exchange Synchronization Configuration.

- The number of saved messages and those in the mailbox memory are determined through synchronization and cannot be manually edited. In order to determine values during synchronization you need to set the parameter ”TargetSystem\ADS\Exchange2000\ReadMailboxSize“.

- Maximum archive size [MB]
  Specify the maximum size of a mailbox‘s personal archive. Warnings are generated once the limit given in <Archive warning from [MB]> is reached.

Booking Resources

The Identity Manager supports properties for booking and planning resource in Microsoft Exchange Server 2010 onwards. The tab <Resource mailbox> for equipment and room mailboxes is also shown.

The following data is shown:

- Automatic processing for meeting requests
  Specify whether automatic calendar processing for resource mailboxes is to be used.

- Resource capacity
  Enter the resource capacity, for example, the number of seats in a meeting room.

- Allow conflicts
  Specify whether overlapping meeting request are permited.

- Allow reocurring requests
  Specify whether a series of meetings is allowed.

- Request only possible during working hours
  Specify whether the resource can be booked during working hours or outside them as well.

- Reject repeating meetings after max. planning period
  Specify whether a series of meeting can be set up such that it exceeds the permitted planning period.

- Forward meeting requests
  Specify whether meeting requests are forwarded to resource mailbox delegates. The delgates decide about the meeting request. Specify delegates using the task <Assign receive restrictions to user accounts> on the tab <Can send as>.

- Max. booking window [days]
  Enter the maximum planning period for meeting request in days.

- Max. duration [min]
  Enter the maximum permitted request period for a resource in minutes.

- Max. conflictíng instances
  Enter the maximum number of conflicts that are allowed for series of meetings that overlap with other meetings. If the value is exceeded, the series request is denied.

- Max. conflict percentage [%]
  Enter a threshold in percent for the permitted conflicts of meetings series that overlap with other meetings. If this value is exceeded, the series request is denied.

- Remove attachments from meeting requests
  Specify whether attachments are deleted from meeting requests.

- Remove comments from meeting requests
  Specify whether message text is delete from meeting requests.

- Remove subject from meeting requests
  Specify whether the subject is deleted from meeting requests.

- Only retain calendar meetings
  Specify whether elements that do not belong the calendar are deleted.

- Add organizer‘s name to subject
  Specify whether the organizer‘s name is given in the meeting request subject field.

- Remove "private" flag from accepted meeting
  Specify whether the state ”Private“ is deleted from meeting requests.

- Mark meeting requests as "Tentative"
  Specify whether meeting requests are marked with the state ”Tenative“ in the calendar. If this option is disabled, meeting requests are marked with the state ”Free“.

- Inform organizer about declined meeting request
  Specify whether the organizer is sent information when a meeting request is declined because of conflicts.

- Send additional information about rejected request
  Specify whether additional information is sent in response to a meeting request. Enter the additional information in the input field <Add additional text>.

- Booking permissions for everyone
  Specify whether meeting requests conforming to policy are automatically approved for all users. If this option is disabled, assign individual users and groups for automatic approval using the tasks <Assign booking authorized user accounts> and <Assign booking authorized groups>.

- Meeting request permissions for everyone
  Specify whether all user meeting requests that conform to policy can be sent. These requests are decided by the mailbox delegate unless the option <Booking permissions for everyone> is set. If this option is disabled, assign individual users and groups for automatic approval using the tasks <Assign meeting request authorized user accounts> and <Assign meeting request authorized groups>.

- Out-of-policy request permissions for everyone
  Specify whether all user accounts can send meeting requests that do not conform to policy. These requests are decided by the mailbox delegate. If this option is disabled, assign individual users and groups for automatic approval using the task <Assign out-of-policy meeting request permission>.

Extended Data for a Microsoft Exchange Mailbox

Enter the user defined schema extensions for the Microsoft Exchange mailbox on the <Extensions> tab.

Additional Tasks for Handling Microsoft Exchange Mailboxes

After you have entered the Microsoft Exchange mailbox master data, you can apply different tasks to the it. You can see the most important information about a group on the overview form. The task view contains different forms with which you can run the following tasks.

Set Up Restrictions on Mailbox Recipients

By default, messages from all users and groups are accepted. You can limit this behavior by using the tasks <Assign receive restrictions to user accounts> and <Assign receive restrictions to groups> to specify the user accounts or groups that messages can accepted or rejected from. These assignments are mutually exclusive. That means you can either specify from whom messages are accepted or you can specify from whom they are rejected. In addition you can specify which users have permission to send messages on behalf of the mailbox owner.

Granting Booking Permissions for Resource Mailboxes

For more information see section Booking Resources.

Assign Distribution Groups for Administration

Use the task <Assign distribution lists for administration> to specify whether the user manages distribution groups. This user can decide on membership in distribution groups. For more information, see section Approving Membership in Distribution Groups.

Assign Moderated Distribution Groups

Use the task <Assign distribution list for moderation> to add user accounts to distribution groups. Use the task <Assign distribution list without moderation> to exclude user accounts from moderation, that means, messages from these user accounts to the distribution group are not moderated. For more information, read section Moderated Distribution Group Extensions.

Disable Mailbox

If a mailbox needs to be disabled, run the task <Disable mailbox>. The mailbox is finally deleted in accordance with retention hold (configuration parameter ”QER\Person\User\DeleteDelay“). Active Directory user accounts with deactivated mailboxes are labeled with the option <Exchange object is locked>.

Administration of Microsoft Exchange Mailboxes via User Account Resources

In order to automatically create a Microsoft Exchange mailbox for a company employee you can implement user account resources. You can create user account resources for each Active Directory domain with Microsoft Exchange. The basic mechanisms are explained in section Creating User Accounts with User Account Resources on page 37.

If an employee needs to obtain the user account through user account resources, the employee has to have a central user account and obtain the IT operating data through assignment to a primary department, primary location or a primary cost center. Refer to the section Handling Employees and User Accounts on page 30.

In the first place, the default installation checks if the employee already has a user account in the user account resource domain. If no user account exists, a new user account is created with the default manage level. If a user account does already exists but is deactivated, it is unlocked.

Creating a User Account Resource for a Microsoft Exchange Environment

Tools: Identity Manager with application role <Target system>/<Active Directory>; Manager

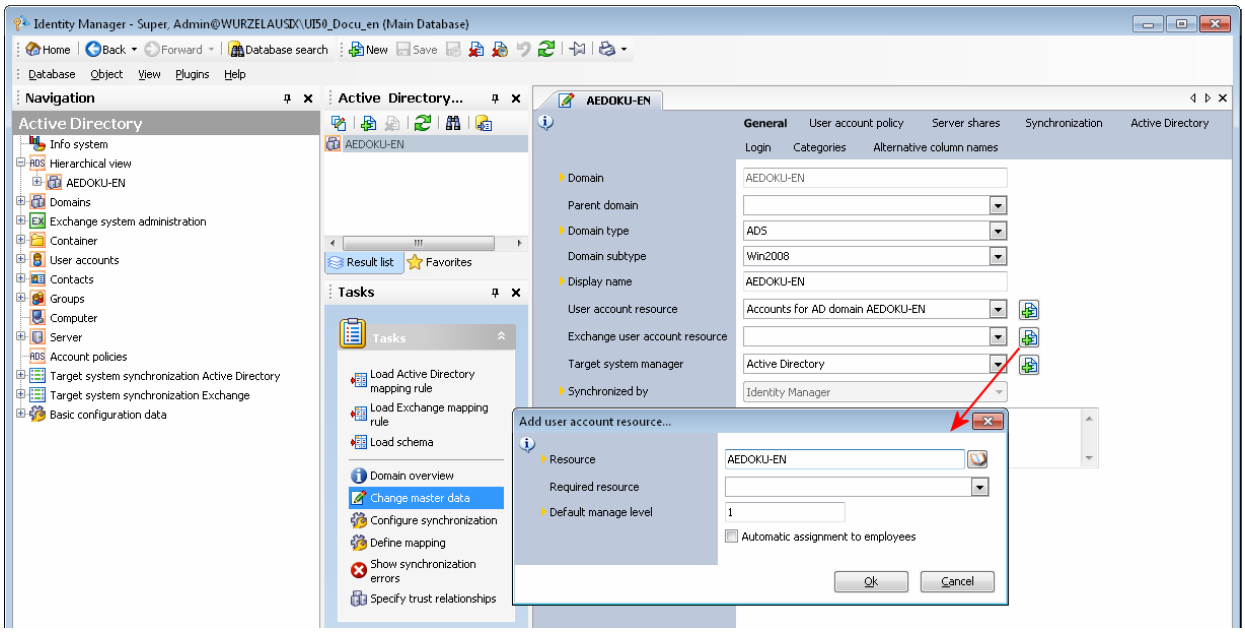
Configuration Paramater for User Account Resources

CONFIGURATION PARAMETER	MEANING
TargetSystem\ADS\Exchange2000\UniqueDefaultManageLevel	When the parameter is set, a different default manage level is expected for each user account resource in the target system (default). If the parameter is not set, each user account resource in the target system may have the same default manage level.

When a Microsoft Exchange user account resource is created a user account resource must already exist for the Active Directory domain because of the integration of Microsoft Exchange functionality in Active Directory.

Create a user account resource for an Active Directory domain with Microsoft Exchange in the category <Active Directory>\<Domains>. Enter a new user account resource on the domain master data form using the button next to the input field.

User Account Resource for an Active Directory Domain with Exchange



Enter the following data for the user account resource:

- The resource name.

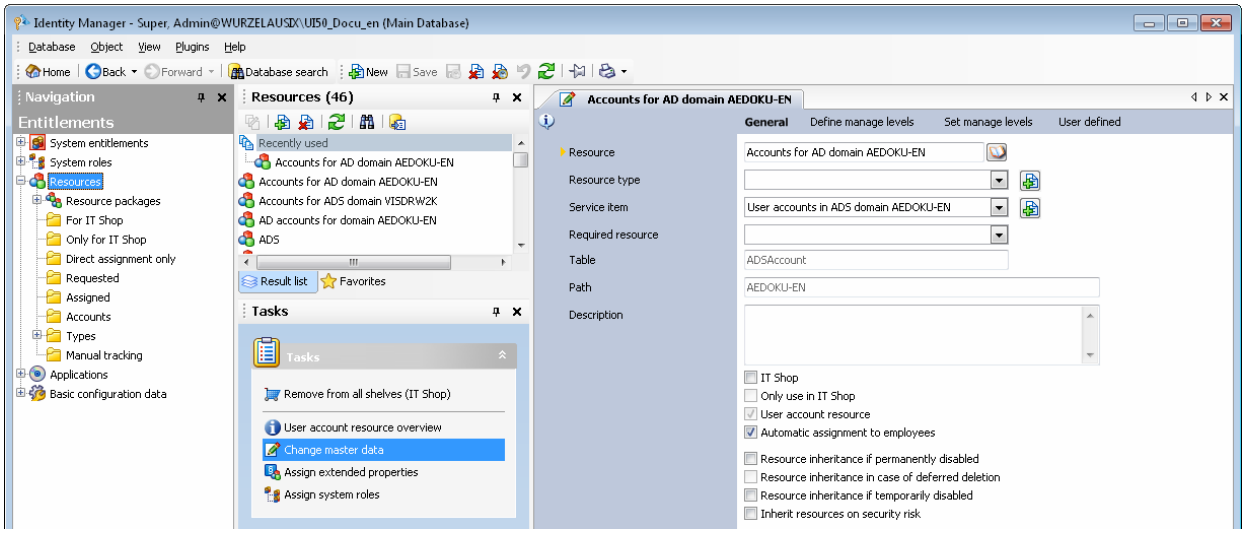
- Default manage level
  Specify the default manage level that will be used when a new user account is added using this user account resource. Enter the value ”1“ to create user accounts in the Identity Manager default installation with a manage level ”Full Managed“. Refer to section Manage Levels for Handling Active Directory User Accounts on page 237.

- Assumed resource.
  Here you can define dependencies between user account resources. This field is left empty for Active Directory domains. Look at section Manage Levels for Handling Active Directory User Accounts on page 237 for more information on creating user account resources for an Active Directory domain.

- Automatic assignment to employees.
  Label the resource with this option if the user account resource should be automatically assigned to all internal employees. The assignment is calculated by the DBScheduler. A new user

account resource is created when the data is saved. Then, you can edit further data for this user account resource in the category <Entitlements>\<Resources> in the filter <Accounts>.

User Account Resource Post-Processing



Addition user account resource data is:

- A resource type.
  Resources should obtain a resource type. This resource type defines future post-processing steps for resource requests or resource assignments. Without a resource type, manual post-processing of an request or assignment is not possible.

- The base table in which the user accounts are displayed
  This data is preset with the table ”ADSAccountMailObject“ when a user account resource is assign to an Active Directory domain and cannot be edited. We are not dealing with a data model table in this case, but an internal mapping view that groups all Exchange relevant information for the table ”ADSAccount“.

- The domain path used by the user account resources
  This data is preset with the NetBIOS name of the Active Directory domain when a user account resource is assigned to an Active Directory domain and cannot be edited.

- Description
  Additional information about the user account resource.

- Service item
  Assign a service item to the resource or add a new one. This way the resource can be internally booked when the resource is requested.

- Specifying for use in the IT Shop
  Label a resource that can be requested through the IT Shop with the option <IT Shop> (see Chapter Setting Up an IT Shop Solution on page 15). This user account resource can be requested by employee via the web front-end and distributed using a defined authorization procedure. The user account resource can still be directly assigned to employees and roles outside the IT Shop. Set the option <Use only in IT Shop> so that the resource can only be requested through the IT Shop. In this case the user account resource can only be requested through th IT Shop.

- Options to deal disabled employee inheritance
  You define the inheritance behavior for each user account resource yourself. The inheritance options of any possible predecessor resources are overwritten. You may want to an employee to inherit a user account resource to, for example, ensure that all required permissions are immediately reinstated for an employee that is reactivated at a later date. User resource account have the options <Resource inheritance if permanently disabled>, <Resource inheritance if temporarily disabled> and <Resource inheritance of security risk> for mapping inheritance behavior. If an employee does not continue to inherit the user account resource when disabled, the user account connected with the employee that was created from this resource assignment is deleted.

The inheritance options of a previous resource are overwritten. If inheritance options are set for the user account resource, the previous resource also inherits, even when it does not have these inheritance options set. A previous resource is removed when the user account resource does not allow resource inheritance.

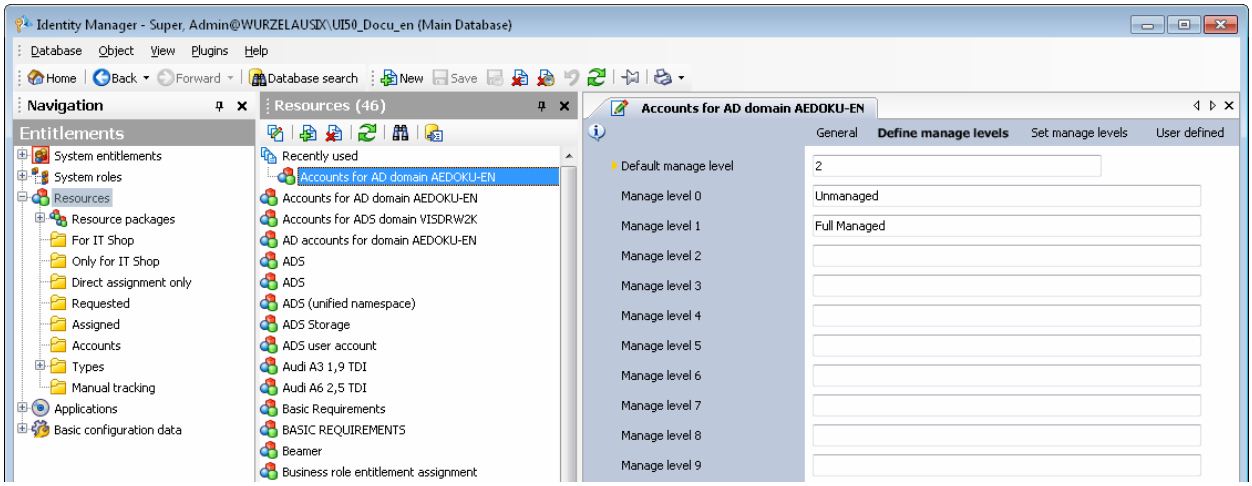
Specifying Manage Levels for Handling Microsoft Exchange Mailboxes

Specify each manage level to deal with Microsoft Exchange mailboxes for a user account resource. The manage level specifies the range of employee properties that are inherited by the user account in the domain.

The Identity Manager supplies a configuration for manage level "Unmanaged" and the manage level "Full managed". These manage levels are taken into account in the templates. User accounts with the manage level "Unmanaged" contain a link to an employee but do not inherit any further properties. User accounts with the manage level "Full managed" inherit defined properties of the assigned employee. You can define other manage levels as you require. You will need to extend the template to accomodate the additional manage levels.

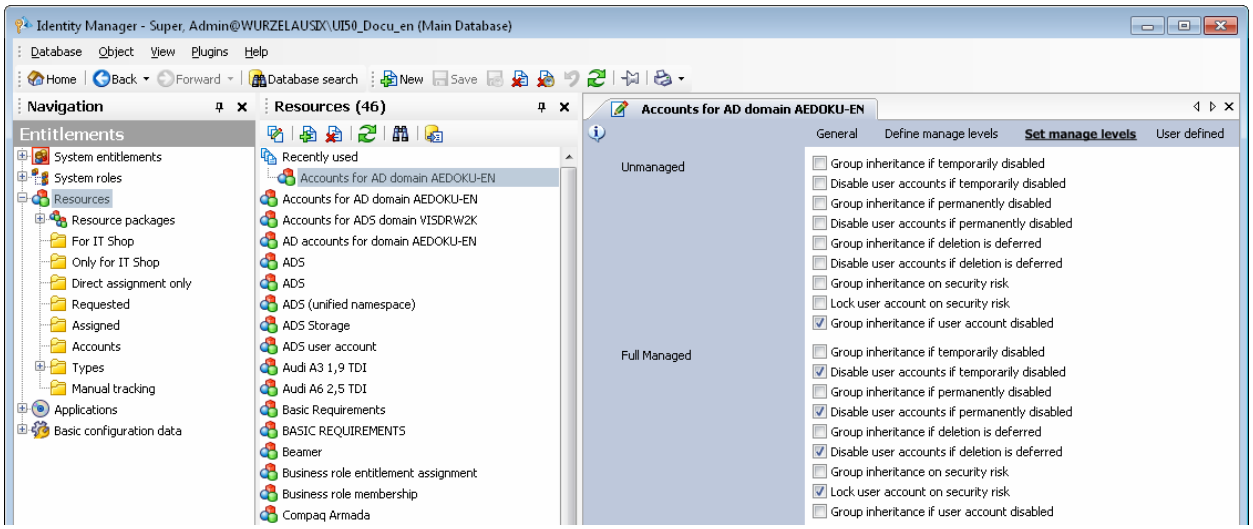
The default manage level is used when mailboxes are added via this user account resource. If several Active Directory domains should be managed with these user account resources you have to create a separate user account resource for each domain. A different default manage level is expected for each target system user account resource in the default installation. However, the Identity Manager does allow several user account resources with the same default manage level to be used. The desired behavior can be controlled via the configuration parameter "TargetSystem\ADS\Exchange2000\UniqueDefaultManageLevel". There is a example in section Creating User Accounts with User Account Resources on page 37 for a more detailed explanation.

Manage Levels for the Microsoft Exchange User Account Resources



Next, you can specify the effects on the user accounts and their group memberships of an employee being temporarily or permanently disabled or deleted for each manage level.

Editing User Account Resource Manage Levels



In order to remove authorizations when disabling or deleting an employee, the employee's mailbox can be locked. If the employee is reenabled at a later date, the mailbox is then unlocked. This behavior is control by the properties:

- Disable user accounts if deactivated permanently
- Disable user accounts if deactivated temporarily
- Disable user accounts if deletion is delayed
- Disable user account on a security risk

Inheritance options for group memberships on employees marked to be disabled or deleted are irrelevant for a Microsoft Exchange user account resource. The inheritance behavior conforms to that of the previous resource setting. Refer to section Manage Levels for Handling Active Directory User Accounts on page 237.

Setting Up Mail-enabled User and Contacts

Tools: Identity Manager with application role <Target system>/<Active Directory>; Manager

You define mail-enabled users in the Manager in the category <Active Directory Service>/<User accounts> and mail-enabled contacts in the category <Active Directory Service>/<Contacts>.

Enabling a Mail-enabled User Account or Contact

Select the Active Directory user account or contact and run the task <Activate Exchange extension>. This displays the input data for the email address setup which can then be edited. The mail-enabled user or contact is created when the modifications are saved.

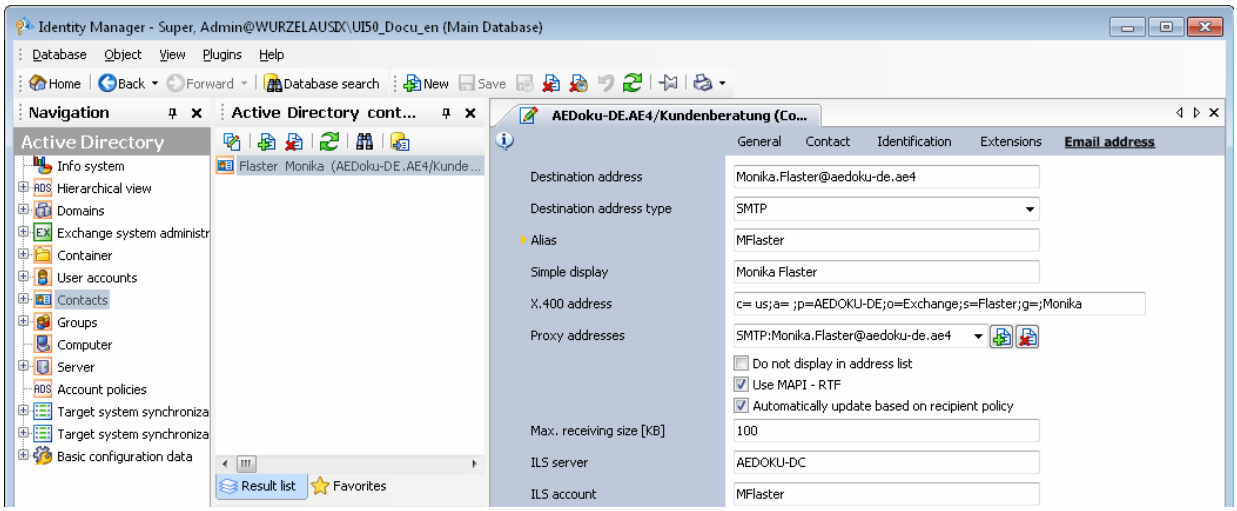
Please note that a user account can either have a mailbox or mail-enable. If a user already owns a Microsoft Exchange mailbox, it has to be disabled first using the task <Disable mailbox>. Then the user can be set up as mail-enabled.

Active Directory user accounts that have have an Exchange extension are labeled with the option <Exchange extension enabled>. If the Exchange extension is disabled, the option <Exchange object is locked> is set.

Master Data for Email Addressing

Enter master data for an mail-enabled recipient on the <Email address> tab.

Setting Up an Mail-enabled Recipient



The minimum requirements for setting up mail-enabled recipients are:

- Destination address and address type
  The destination address data includes the target address and the destination address type. Enter a forwarding address for messages. You can also add other mail connectors (e.g. CCMail, MS) apart from the standard destination address type (SMTP, X400).

- Issuing an Alias
  The alias should be unique and is used to identify the mail-enabled recipient.

Additional data:

- Simple display name
  The simple display name is used for systems that cannot interpret all the character of a normal display name.

- Addressing in X400 format and proxy addresses
  Enter the email addresse in X400 format in the <X400 address> input field for addressing the mail-enabled recipient. In the input list <Proxy addresses> you can add further email addresses to the mailbox. You can also use other mail connectors (e.g. CCMail, MS) as address types for default addressing (SMTP, X400). The following syntax should be observed for setting up other proxy addresses:

  ```
  Adress type: new email address
  ```

- Displaying in address book
  Set the option <Do not display in address list> on the mailbox if you want to prevent the mailbox being displayed in address lists. This option is valid for all address books.

- MAPI RTF
  Set the option <Use MAPI-RTF> when the mail-enabled recipient is allowed to receive messages in MAPI format.

- Automatic update depending on recipient policy
  Set the required options if the changes to the user's email address should be updated automatically based on recipient guidelines.

- Maximum receive size [KB]
  Specify the maximum size (in KB) for messages that the mail-enabled user may send or receive. The Exchange organization global settings in the Exchange Manager come into effect for message delivery if there are no limitations.

- Online list information
  Enter the ILS server and ILS account user or contact for the online list information about the mail-enabled recipient.

- Assistant (only for mail-enabled user accounts)
  An assistant can be named in the input field <assistant name> or <Assistant>. The assistant is is displayed in the email recipient's properties in Microsoft Outlook. You can use any characters for the assistant name. The name is mapped to the attribute "msExchAssistantName" in Active Directory. From the Microsoft Exchange Server 2003 onwards, the assistant is determined by its distinguished name and is mapped to the "Secretary" attribute in Active Directory.

Extended Data for Mail-Enabled Recipients

On the <Extended> tab you can enter user defined additions for mail-enabled recipients.

Additional Tasks for Managing Mail-enabled Recipients

After you have entered the mail-enabled recipient master data, you can apply different tasks to the it. You can see the most important information about a group on the overview form. The task view contains different forms with which you can run the following tasks.

Set up Recipient Limitations for Mail-enabled Users

By default, all user and group messages are accepted. You can limit this behavior by using the tasks <Assign receive restrictions to user accounts> and <Assign receive restrictions to groups> to specify the user accounts or groups that messages can accepted or rejected from. These two assignments are mutually exclusive. That means, you may either specify from whom messages can be accepted or specify from whom they can be rejected. In addition, you can define which uses has the right to send messages on behalf of the mailbox owner.

Granting Booking Permissions for Resource Mailboxes

For more information see section Booking Resources.

Assign Distribution Groups for Administration

Use the task <Assign distribution lists for administration> to specify whether the user manages distribution groups. This user can decide on membership in distribution groups. For more information, see section Approving Membership in Distribution Groups.

Assign Moderated Distribution Groups

Use the task <Assign distribution list for moderation> to add user accounts to distribution groups. Use the task <Assign distribution list without moderation> to exclude user accounts from moderation, that

means, messages from these user accounts to the distribution group are not moderated. For more information, read section Moderated Distribution Group Extensions.

Disable a Mail-Enabled Recipient

If a mail-enabled recipient needs to be disabled, run the task <Disable email address>. The recipient is finally deleted in accordance with retention hold (configuration parameter ”QER\Person\User\DeleteDelay“). Active Directory user accounts with disabled email addressing are labeled with the option <Exchange object is locked>.

Mail-enabled Groups

Tools: Identity Manager with application role <target system>/<Active Directory>; Manager

Set up mail-enabled groups (subsequently distribution groups) in the category <Active Directory>\<Groups>.

From Microsoft Exchange Server 2007 and later, only universal security groups, universal distribution groups and dynamic distribution groups can have mail-enable.

Enabling and Disabling a Distribution Group

Select an Active Directory group and run the task <Activate Exchange extensions>. This displays the input data for the email address setup which can then be edited. The distribution group is created when the modifications are saved. In order to delete mail-enabling at a later date, run the task <Disable distribution lists>.

Email Addressing Master Data

The following list describes the relevant master data for email addressing of Active Directory groups. You can find details of Active Directory specific master data in section Entering Master Data for Active Directory Groups. Enter master data for distribution group mail-enable on the <Exchange> tab (unless directed otherwise).

The minimum requirements for mail-enabled distribution group are:

- Distribution group email address
  Enter the email address on the <General> tab.

- Alias
  The alias should be unique and provides further identification for the distribution group.

- Simple display name
  The simple display name is used for systems that cannot interpret all the characters of the normal displayname.

- Expansion server data
  Enter a server on which the distribution group should be expended. If you set the option <All site servers>, the distribution group is copied to all servers.

Additional data:

- Addressing in X400 format and proxy addresses
  You can also use other mail connectors (e.g. CCMail, MS) as address types for default addressing (SMTP, X400). The following syntax should be observed for setting up other proxy addresses:

  ```
  Adress type: new email address
  ```

- Automatic updated based on recipient policies
  If changes that are made to a recipients email address based on the recipient policy need be automatically updated, set the corresponding option.

- Show in address book
  Set the option <Do not display in address list> on the mailbox if you want to prevent the mailbox being displayed in address lists. This option is valid for all address books.

- Do not show membership in distribution groups
  Set this option if distribution list memberships are to be shown.

- Maximum receive size [KB]
  You can specify the maximum size (in KB) of message that can be received by the distribution group. If no limits are given, the globally defined settings for Exchange organization message handling in the Exchange System Manager come into effect.

- Only limit messages from authenicated users (Microsoft Exchange Server 2007 or later)
  Set this option if only messages from authenticated users are permitted.

- Out-of-office message to sender (Microsoft Exchange Server 2010 or later)
  Set this option if the message sender should receive out-of-office messages.

- User defined schema extension for the distribution group
  These are entered on the <Extensions> tab.

Extensions for Dynamic Distributions Groups

Dynamic distribution groups can be set up in Microsoft Exchange Server 2007. The members of a dynamic distribution group are not fixed but are determined using a filter criteria. Load dynamic distribution groups into the Identity Manager using synchronization and only edit them if necessary.

The following additional data is displayed for dynamic groups:

- Object class
  The object class is shown on the <General> tab. The value ”MSEXCHDYNAMICDISTRIBUTIONLIST“ is expected for dynamic distribution groups.

- Recipient base container
  The condition for finding distribution group members is applied to the selected Active Directory container and its subcontainers.

- Condition
  The condition contains a filter criterion, which is used to determine the members of the distribution group.

- Data specifies which recipient types are allowed
  Select the option <All recipient types> to allow every recipient type. Use the options <Contact with email address>, <Groups with email address>, <User accounts with email address>, <User accounts with mailbox> and <Resource mailboxes> to limit recipient types.

Approving Membership in Distribution Groups

As from Microsoft Exchange Server 2010, membership in distribution groups can be applied for and approved. The following task are available to do this:

- Add to group
  Use this option to specify which members can be part of the distribution group. Following values are permitted:
  Open - members can be added to the group without approval.
  Closed - only distribution group administrators can add members to the group. Requests to be added to the group are automatically denied.
  Shared by owner - requests to be added to the group can be made and are approved by the distribution group administrator.

- Leave group
  Use this option to specify how members can leave the distribution group. Following values are permited:
  Open - member can leave the group without approval
  Closed - member can only leave the group with approval from the administrator. Requsets to leave the group are automatically denied.

Use the task <Assign distribution list administrator> to specify which users manage the distribution group and therefore can grant approval about membership in the group.

Moderated Distribution Group Extensions

As from Microsoft Exchange Server 2010 moderated distribution groups are let a moderator approve or deny messages sent to distributed group. Only after a message has been approved by a moderator can it be forwarded to members of the distribution group. Read the documentation from your Microsoft Exchange Server on the concept of moderated distribution groups.

The following data is shown for moderated distribution groups in addition:

- Distribution list moderation
  Set this option if the distribution group should be moderated. Use the task <Assign moderators> to specify moderators for the distribution group.

- How senders are notified when they send messages to moderated distribution groups.
  Set the option <Do not notify> if the sender should not be notified. Set the option <Only notify senders in your exchange organisation> if only internal sender should be notified. Set the option <Notify all senders> if internal and external sender should be notified.

Use the task <Exclude user accounts from moderation> and <Exclude distribution lists from moderation> to specify the user accounts and distribution groups whose messages to moderated distribution groups are exluded from moderation. Use the task <Excluded from moderation in> to select groups that contain distribution groups that are excluded from moderation.

Additional Tasks for Managing Distribution Groups

After you have entered the distribution group master data, you can apply different tasks to the it. You can see the most important information about a group on the overview form. The task view contains different forms with which you can run the following tasks.

Recipient Limitations for Setting Up Distribution Groups

By default, all user and group messages are accepted. You can limit this behavior by using the tasks <Assign receive restrictions to user accounts> and <Assign receive restrictions to groups> to specify

the user accounts or groups that messages can accepted or rejected from. These two assignments are mutually exclusive. That means, you may either specify from whom messages can be accepted or specify from whom they can be rejected.

Assigning Distirbution Group Managers

Read section Approving Membership in Distribution Groups on page 293 for more information.

Configuring Distribution Group Moderation

Read section Moderated Distribution Group Extensions on page 293 for more information.

10

Managing a Lotus Notes Environment

- Introduction
- Lotus Notes Synchronization Procedure
- Setting Up Lotus Notes Sychronization
- Basic Configuration Data
- Lotus Notes Certificate
- Lotus Notes Templates
- Lotus Notes User Account
- Lotus Notes Groups
- Mail-In Databases
- Lotus Notes Servers

Introduction

In an Identity Manager database, it is possible to manage several productive Lotus Notes environments in parallel by defining Lotus Notes domains. Lotus Notes environment objects such as users, groups, mail-in databases, servers and certificates can be administrated with the Identity Manager.

To certify a new user, he or she requires a set of user specific data for Lotus Notes to be generated on the local PC (i.e. in the home directory) in order to work with Lotus Notes. When a new user is added in the Identity Manager, the user ID file for authentication, the mailbox file and the personal address book are created for the user.

The Identity Manager provides company employees with the necessary user accounts. You may use different mechanisms for connecting employees to their Lotus Notes user accounts. It is also possible for you to manage Lotus Notes user accounts separately from employees and, therefore, set up administrative user accounts.

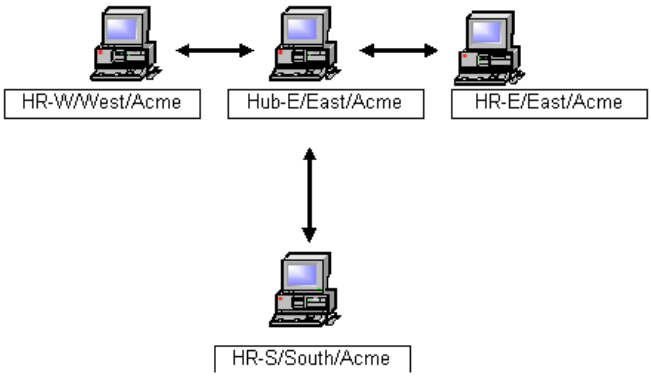
Lotus Notes groups and mail-in databases are managed along side Lotus Notes user accounts in the Identity Manager. Lotus Notes groups are used to supply users, servers and groups with the necessary access permissions. User messages can be sent over the jointly used mail-in databases. Users can access these mail-in databases when permissions have been issued. When a mail-in database is added using the Identity Manager, the necessary mailbox file is created.

Lotus Notes servers and certifications are only read into the Identity Manager database so that they can be referenced by users and groups. The Identity Manager access lists can be defined for server documents in order to specify who has access to a server for what reason.

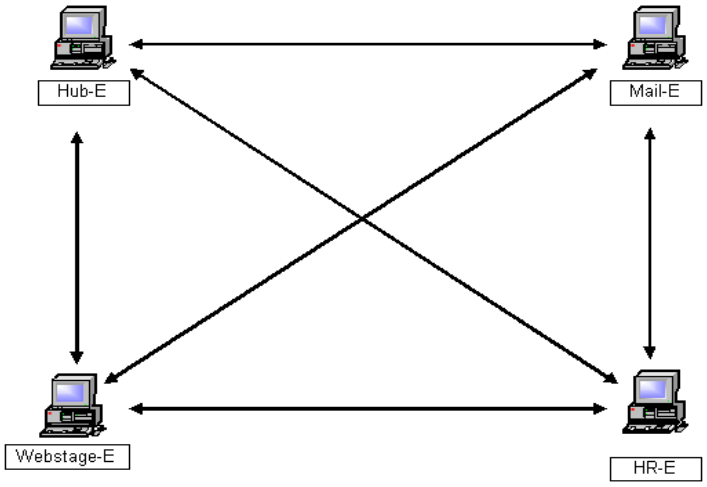
Lotus Notes Synchronization Procedure

A Lotus Notes domain consists of one or more Lotus Notes servers. These servers replicate the primary Domino Directory (in a hub and spoke or peer-to-peer schema). Changes are only made on the central server. This is normally the central hub in a hub and spoke topology or an arbitarily specified server in a peer-to-peer topology. The Domino Directory contains all documents for certificates, groups, mailbox files, user, servers and other configuration documents.

Hub and Spoke Topology



Peer-to-Peer Topology



A server is defined within the Identity Manager environment to execute all administrative task effecting the Lotus Notes environment. This server is named the gateway server in the rest of this chapter.

The gateway server cannot be a productive Lotus Notes server itself but requires access to the Lotus Notes servers in the productive environment. Identity Manager Service is installed on the gateway server with Lotus Notes synchronization components and the Notes database ”viAgentDB.nsf“ provided by us.

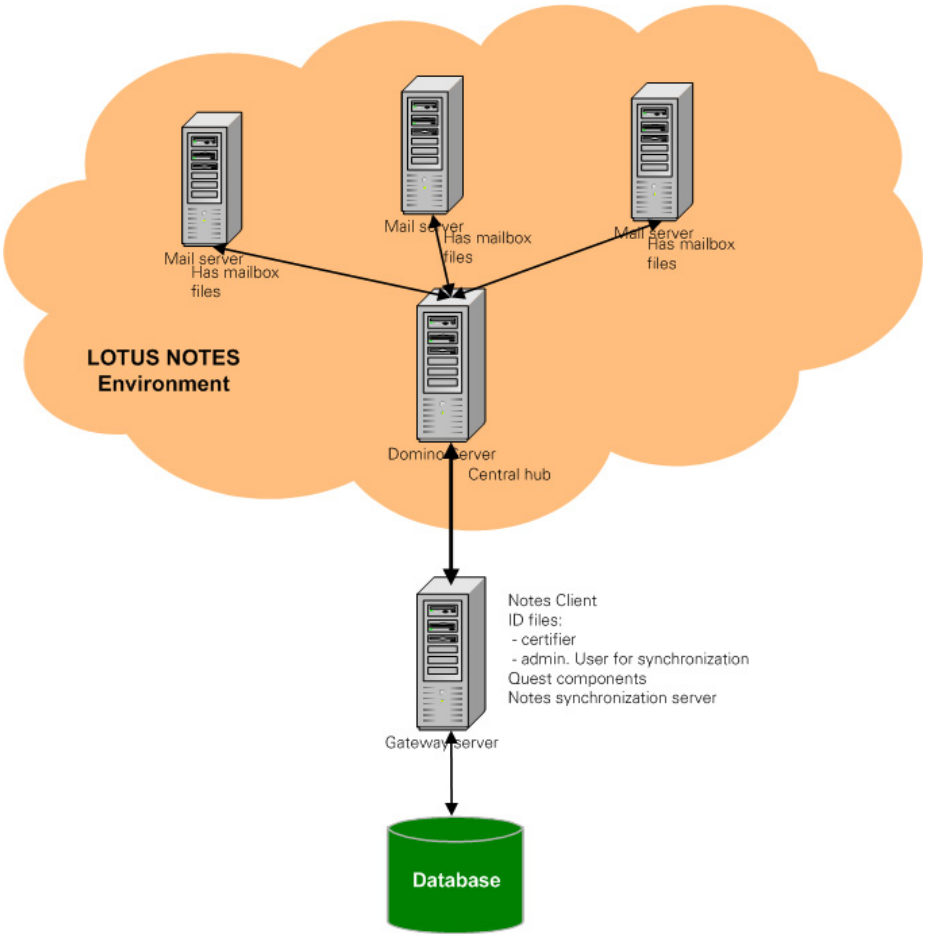
On the user side, an ID file has to exist with sufficient administrative rights for accessing the productive Lotus Notes environment on synchronization. A certification ID file also has to be supplied. Both files must be available on the gateway server.

The gateway server communicates with a domino server when actions are carried out on the productive address book and mailbox file. This domino server is a selected productive Notes server with a good network connection to the gateway server. All synchronizer actions are executed from the gateway server. The entries that are of interest for synchronization and administration with the Identity Manager database (certficates, servers, groups, mailbox files, users, mail-in databases, ID files) are processed by the getway server.

The gateway server uses Identity Manager Service to execute functions such as adding, changing and deleting Notes users and groups on the domino server. In addition to this, databases can be also added to Lotus Notes servers as Notes users, mailbox files or mail-in databases. The actual functions are implemented within the Lotus Notes agent (script) ”viAgentsDB.nsf“. The parameters are exchanged using a so-called context document. The Notes client context and all the necessary data exchange func-

tions for executing Notes agents and for error handling are included in the context document supplied by Identity Manager Service.

Domino Server Access



Setting Up Lotus Notes Sychronization

Identity Manager Service is responsible for comparing information between the Identity Manager database and the Lotus Notes environment. Synchronization prerequisites are:

- Installation and Configuration of a gateway server
- Setting up the database for syynchronization

The basic synchronization mechanisms are explained in the chapter Data Synchronization in Identity Manager on page 161.

Installation and Configuration of a Gateway Server

To set up a gateway server, a computer has to be available with the following software installed on it.

- Windows 2000 Server or Advanced Server with Service Pack 2 or later for Windows 2000, Windows Server 2003, Windows Server 2003 R3, Windows Server 2008 or Windows Server 2008 R2

- Microsoft .NET Framework with version 3.5 or later, service pack 1
- Microsoft Software Installation (MSI) service
- Write access to ”C:\Lotus\Notes“ and the Identity Manager installation directory.

Special Requirements for Synchronizing a Lotus Domino 8.5. Environment

The following versions of Lotus Notes and Lotus Domino Components are an absolute minimum prerequisite for synchronizing a Lotus Notes Domino 8.5. environment.

- Lotus Notes Client on the Gateway in version 8.5.1 with fixpack 2
- Lotus Domino Server version 8.5.1 with fixpack 2

Lotus Notes Client Installation

There has to be a Lotus Notes Client (at least version 6) installed on the gateway server with the following configuration.

- Installation directory: C:\Lotus\Notes
- Extend PATH variable to include ”C:\Lotus\Notes“ and ”C:\Lotus\Notes\Data“
- Certified ID file is stored for maintaining the certificate.
- Domino directory certificate document has been copied to the personal address book of the syncnronization administrator. See section How to Copy the Lotus Notes Certificate on page 301 for more information.
- ”VIAgentsDB.nsf“ and ”VICustomDB.nsf“ exist in directory C:\Lotus\Notes\Data . You find these files on the Identity Manager install CD in the directory ”...\Redistributables\Notes“. ViAgentsDB.nsf must have a signature as according to section viAgentsDB.nsf Signature on page 303.
- Customize the VINotes.ini according to section Customizing VINotes.INI on page 303.

The directory ”C:\Lotus\Notes“ must be selected as the destination directory! The directories for storing the ID files (”C:\Lotus\Notes\Data\IDS\<Domainname>“) and the mail files (”C:\Lotus\Notes\Data\Mail“) for the user are subsequently set up.

Enter the Lotus Notes install path, that means the path where ”Notes.exe“ can be found (”C:\Lotus\Notes“), in the default search path for the operating system (PATH variable). When the Lotus Notes Client is installed, the path selected for the Notes data directory should also be added (”C:\Lotus\Notes\Data“).

A certifier ID file needs to available on the gateway server in preparation for registering user using the certificate. The certifier ID file may only be created with one password.

Prerequisite for succesfully running the ”rename“ and ”recertifying“process is the existance of the certification log database (certlog.nsf).

Preparing User Accounts for Synchronization

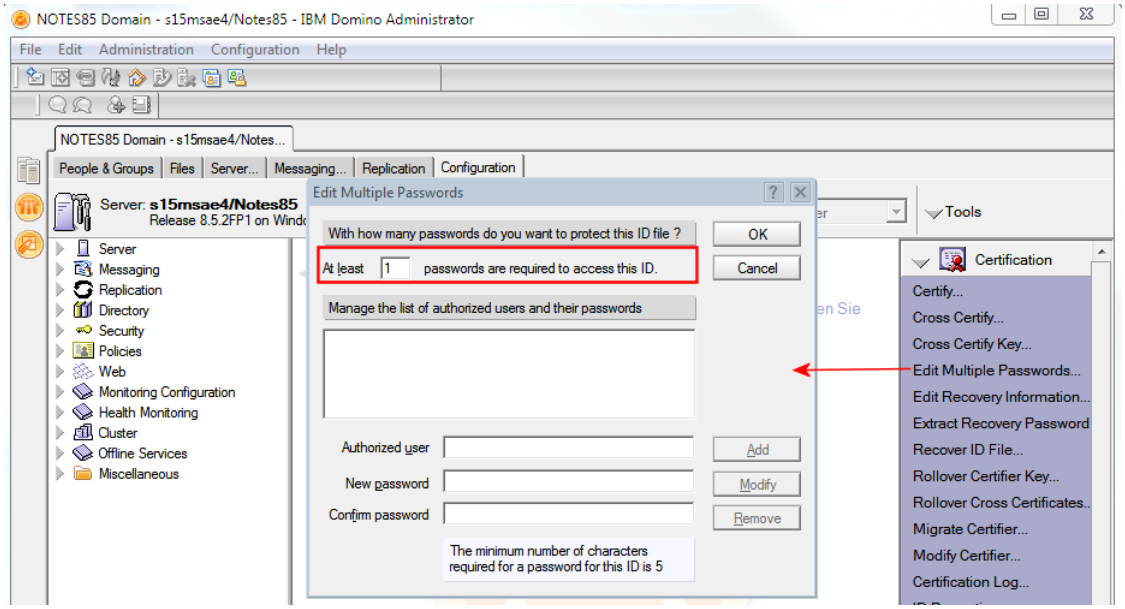
The synchronization administrator needs sufficient administrative permissions for the primary Domino directory (names.nfs). The minimum requirements are:

- Access function ”Manager“ on the primary Domino directory
- Permissions for deleting documents
- Access to an Domino environment administration server (server on which it is possible to register a new user and create AdminP requests).
- All roles

Furthermore, you need to configure the regional date setting (short date format) for the Identity Manager Service user account on the gateway server. The date format on the gateway server always needs to be in U.S. format (e.g. mm/dd/yyyy).

After successful installation, an ID file for the user needs to be added under the directory ”C:\Lotus\Notes\Data“ for synchronization. The ID file for this user should be supplied by the customer. This ID file is created with a single password. Multiple passwords are not supported. The password options are checked in Lotus Domino Administrator under ”<Server>/<Configuration>/<Certificates>“.

Notes Administrator - Checking Password Options



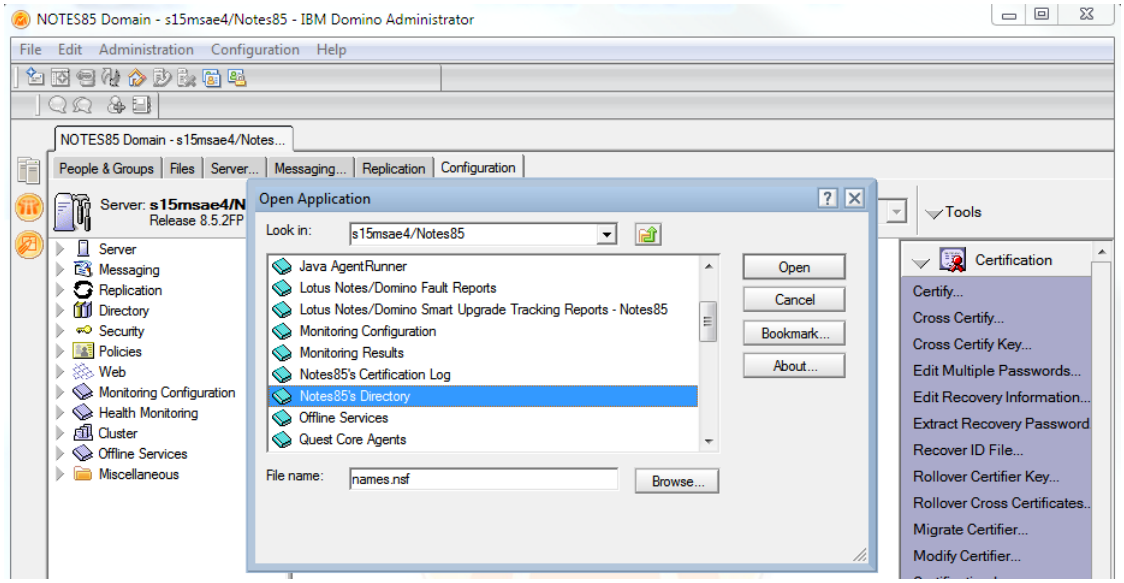
The administrator ID file that is created when the Notes server is installed may not be used because it is used for other administrative tasks.

Subsequently, the Lotus Notes client should be started with the administrator’s ID file for accessing the productive environment and the first login is carried out. This causes the configuration entries on the computer. The access rights can be checked by calculating a new Notes user with the ID file as a test.

How to Copy the Lotus Notes Certificate

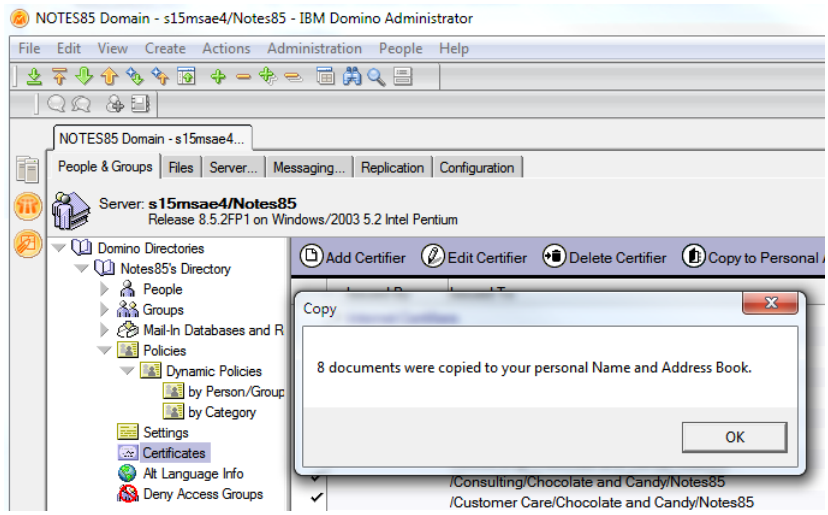
When you are configuring the gateway server ensure that the Lotus Notes certification document is copied from the Domino server address book into the administrators personal address book for synchronization. This is required to guarantee exchanging Lotus Notes user account account certifiers from the Identity Manager. To do this, start the Lotus Notes Client with the administrator synchronization user account. Select the server from the menu <File>\<Application>\<Open> and open the address book (names.nsf).

Opening the Address Book Saved on the Server



Then you open the certificate view and mark the Lotus Notes certificate document. Use the entry <Copy to personal address book> to start the certifcate document copy.

Copying the Lotus Notes Certificate Document

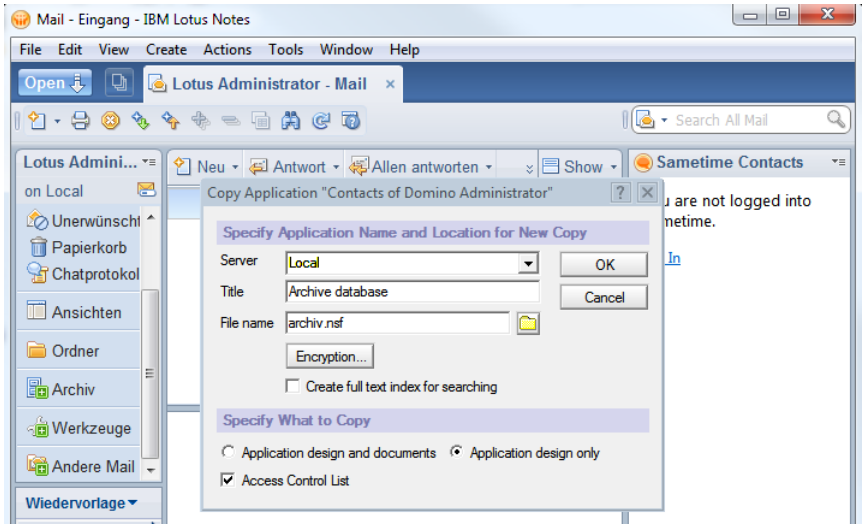


Setting up an Archive Database for backing Up Employee Documents

When you add a new Lotus Notes user account in the Identity Manager, a copy of the initial user document is copied to an archive database on the gateway server. This archive database is added at the begining and should be part of a daily back up.

The fastest method of adding an archive database is to create an empty copy of the local address boolk on the gateway server. To do this, open the local address book in the Lotus Notes Client on the gateway server and select the menu item <File>\<Application>\<New Copy> to create a copy. Use the name ”Archiv.nfs“ for the database as the Identity Manager processes use it. Furthermore, the option <Database Design only> has to be selected so that an empty database is generated.

Creating a Copy of the Database



After the copy operation has completed, the ”archiv.nfs“ can be found in the installation data directory (”c:\Lotus\Notes\Data“).

Identity Manager Services Installation and Configuration

The installation of Identity Manager Service on the gateway server in described in section Installing Identity Manager Tools on page 23. Take note of the installation advice about installing on a terminal server (see Installing on a Microsoft Windows Terminal Server on page 25).

After the installation has been successfully completed, the files ”VINotes.INI” and ”NotesEM.DLL” should be available in the directory ”C:\Lotus\Notes“. ”VINotes.INI“ needs to be modified before synchronization. See section Customizing VINotes.INI on page 303 for more information.

Furthermore the file ”VIAgentsDB.NSF“ can be found in the directory ”C:\Lotus\Notes\Data“ after Identity Manager Service’s installation. This file has to be labeled before synchronization. For more information see section viAgentsDB.nsf Signature on page 303.

Once the file ”VINotes.INI“ and the signature for the file ”VIAgentsDB.nsf“ have been customized, configure Identity Manager Service on the gateway server and start the service. For more information see section Setting Up a Server for Database Access on page 44.

Customizing VINotes.INI

The file ”VINotes.INI“ is an image of the ”Notes.INI“ file, which is created when the Lotus Notes client is configured. When Identity Manager Service is updated, VINotes.INI is overwritten! Therefore, it makes sense to create a backup copy of the customized ”VINotes.INI!

VINotes.INI is customized by copying the contents of Notes.INI to VINotes.INI. The Notes.INI can remain as such. Enter the name of the administrator’s ID file in VINotes.INI and change it there. Please note that VINotes.INI has to contain the following keys in the ”[Notes]“ section:

Directory	Path to the Notes data directory (local directory)
KeyFileName	Path for user ID file that should be used (local directory)
EXTMGR_ADDINS	Name of extension DLLs, in this case NotesEM.dll
KitType	Specify the Notes type 1= client, 2= server

Example VINotes.INI

```
[Notes]
Directory=C:\Lotus\Notes\data
KeyFilename=custom.id
KitType=1
Timezone=-1
DST=1
EXTMGR_ADDINS=NotesEM.dll
$$HasLANPort=1
```

After successfully changing VINotes.INI a function test should be carried out. The following line needs to be commented out and the login should be be made with VINotes.INI.

```
EXTMGR_ADDINS=NotesEm.dll
```

After a successful login, the comments should be removed again.

viAgentsDB.nsf Signature

When Identity Manager Service is installed it supplies a Lotus Notes database ”viAgentsDB.NSF“, which contains agents for accessing the productive Lotus Notes address book and for creating ID files. The objects in this database are given a signature by Quest Software that is not valid in the customer’s environment. This file has to be signed by the Lotus Domino administration with a signature from the customer environment before synchronization can go into start. (View <Files>, context menu <Sign>).

Without a signature, user ID files created with this database are not automatically recognized and a valid signature is requested at the first login.

The Identity Manager Database Synchronization Setup for Lotus Notes

Configuration Parameters for Lotus Notes Environment Synchronization

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes	Lotus Notes is supported. Preprocessor relevant configuration parameter. Changes to the parameter require recompiling the database.
TargetSystem\Notes\Accounts	Settings for handling Lotus Notes user account accounts come into effect.
TargetSystem\Notes\Accounts\InitialPassword	Preset initial password for new user accounts.
TargetSystem\Notes\MaxFullsyncDuration	Specifies max runtime for a synchronization.
TargetSystem\Notes\PersonAutoFullsync	This parameter specifies whether automatic assignment of employees should come into effect when a user account is added during synchronization.
TargetSystem\Notes\ReadMailfileSize	The user mailbox file parameters are loaded into the database during synchronization.
TargetSystem\Notes\RedoDelay	This configuration parameter specifies the delay time after which an incompleted update is repeated. The input is in minutes.
TargetSystem\Notes\RestoreMode	Determines the delta set resulting from sychronization of the Identity Manager database and the target system Lotus Notes.
TargetSystem\Notes\RestoreMode\AutoDelete	The database superset is deleted by synchronization methods ”CompareAndInsert“ and ”CompareAndUpdate“ if the configuration parameter ”TargetSystem\Notes\RestoreMode“ has a value of 0.
TargetSystem\Notes\ServerVersion	Supplies the version of main release Lotus Notes client installation on the gateway server that is required for registering new Lotus Notes user accounts amongst others.
TargetSystem\Notes\SetDefaultNotesDomain	When this parameter is set, a foreign key relation is created for the most recently compared ”NotesDomain“ in the Identity Manager database Notes objects ”NotesUser“ and ”NotesMailInDB“ provided there is no value in the parameter corresponding to this object.
TargetSystem\Notes\SyncObjects	The child configuration parameters specify which objects are to be sychronized between the target system environment and the database. You can find a complete list of configuration parameter in the Configuration Manual.
TargetSystem\Notes\UseUSN	A USN comparaison is run when Notes objects are synchronized.

Configuration Parameters for Lotus Notes Environment Synchronization

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\VerifyMemberships	The object properties are tested each time an object is added/inserted. If the properties in the target system are different from those in the database, the process steps which write properties to the target system are rerun. The parameter is valid for all object types that do not have a VerifyUpdate parameter under the configuration parameter ”TargetSystem\Notes\RestoreMode“. If the parameter is not set, testing does not take place.

Prerequisites for synchronizing a Lotus Notes environment with the Identity Manager database are:

- Setting the configuration parameter for synchronization with Lotus Notes
  The configuration parameter ”TargetSystem\Notes“ is a preprocessor relevant configuration parameter. This means that the database has to be compiled after changing this parameter. For more information read the section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual. Specify which Lotus Notes objects are to be sychronized between the target system environment and the database using the configuration parameter below ”TargetSystem\Notes\SyncObjects“.

- Declare the gateway servers
  Refer to section Declaring the Gateway Server on page 306.

- Declare the Lotus Notes domain to synchronize in the Identity Manager
  This procedure is described in section Declaring the Domino Servers in the Identity Manager Database on page 309.

- Declare Domino Server (Notes central hub)
  This procedure is described in section Declaring the Domino Servers in the Identity Manager Database on page 309.

- Configure and enable scheduled tasks

- Customizing the certificate (path for certifier ID file, password for file)
  The certificates are read in at synchronization. If users are going to be registered using the certifcate the full! file path for the ID file on the gateway server must be entered into the Identity Manager database after initial synchronization. The certifier ID file has to provided by the customer.

Target System Wizard for the Identity Manager Database Synchronization with Lotus Notes

On the Manager home page, there is a wizard to help set up the Identity Manager database to synchronize with a Lotus Notes environment. The assistant includes the most important configuration steps for putting synchronization into operation. The wizard takes you through the configuration steps from setting up the Lotus Notes domain in the Identity Manager database through to synchronization. The synchronization does not include all objects but only those that are earmarked for continued use. Basically, the assistant does not make any settings to Notes that are managed by the Identity Manager. All settings are changes to the Identity Manager behavior and are saved in the Identity Manager database.

The following steps are carried out by the wizard:

- Set up a gateway server in the database

- Set up a Lotus Notes domain in the database
- Set up a Domino Servers in the database
- Start the initial synchronization for the Lotus Notes environment

After the wizard is completed, other configuration steps may be necessary in order to manage the Lotus Notes environment in the Identity Manager.

Declaring the Gateway Server

Tools: Manager; Identity Manager with application role <Target systems>/<Lotus Notes>

Configure new synchronization servers in the category <Lotus Notes>\<Server>. A minimum of the following data has to entered for a synchronization server:

- Server
  Server name
  The server name is used to compose the queue name for the corresponding Job server. The process steps are requested in the Job queue with exactly these queue names.
- Hardware
  Name of the hardware that the synchronization server is installed on.
- Language
  Language setting for the synchronization server
- Label as Lotus Notes Gateway Server

This input does not, however, have any meaning for the function of the server as synchronization server.

Once the synchronization server has been added to the database, a corresponding entry is made for a Job server that supplies the queu for handling the target system specific processes through Identity Manager Service. Enter the queue in the Identity Manager Service configuration file. For more information read section Configuring a Job Server on page 210 in the Configuration Manual.

Lotus Notes Domain Setup in the Identity Manager Database

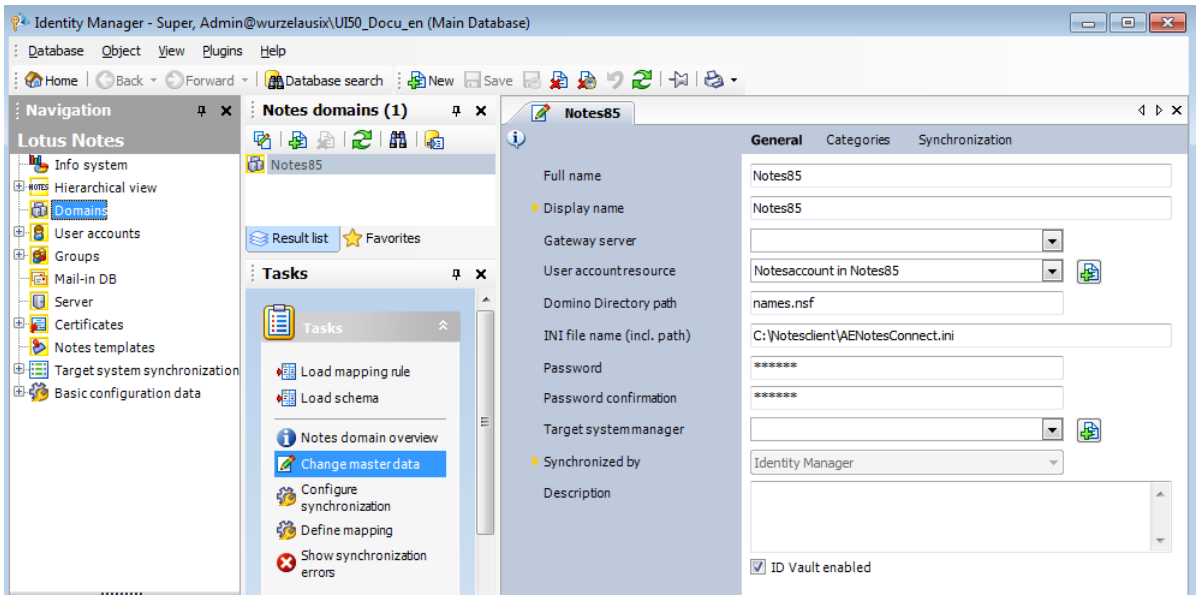
A Lotus Notes domain in the Identity Manager corresponds to a the image of a specific area in Lotus Notes, for example a productive Lotus Notes environment. Using this construction, that is far more stringently handled in the Identity Manager than in Lotus Notes, it is possible to manage several productiv Lotus Notes environments in parallel with an Identity Manager database.

Even when the relationship of a Lotus Notes user account to his or her domain is not maintained in Lotus Notes, the Identity Manager is able to match the current Lotus Notes domains from the Domino server to be read in (see configuration parameter ”TargetSystem\Notes\SetDefaultNotesDomain“) and therefore to separate the environments.

General Master Data for a Lotus Notes Domain

Lotus Notes domains are declared in the Manager in the category <Lotus Notes>\<Domains>.

Setting Up a Lotus Notes Domain



Enter the required data for a Lotus Notes domain on the form <Change master data>.

You need to enter at least the following information for the domain:

- Full name of the Notes domain to be synchronized
- The gateway server
  Enter the gateway server that is going to run the synchronization with the Lotus Notes environment. All servers that are marked with the option <Lotus Notes Gateway server> are supplied in the selection list.
- The Notes address book
  Enter the name of the primary Domino Directory (Names.nsf) from the domino server here.
- Path to Notes.INI file and the name of the INI file (vinotes.ini)
  If the gateway server is installed following the recommendations in section Installation and Configuration of a Gateway Server on page 298, the viNotes.ini is in the directory ”C:\Lotus\Notes“ by default. This Lotus Notes client control file contains Quest Software’s own extensions necessary for correctly creating new Lotus Notes user accounts as well as data for authenication on a Lotus Notes system.
- Password input
  Enter the password for accessing the primary Domino Directory using the administrator’s ID file for synchronization. Enter the name of the user ID file in the viNotes.ini file on the gateway server.
- User account resources
  This data is required when Lotus Notes user account accounts are managed through a user account resource in the target system. You can read more in the section Managing Lotus Notes User Accounts with User Resource Accounts on page 324.

- Synchronized by
  Specify how the data will be synchronized between the Lotus Notes domain and the Identity Manager. Choose between ”Identity Manager“, ”FIM“ and ”No synchronization“.

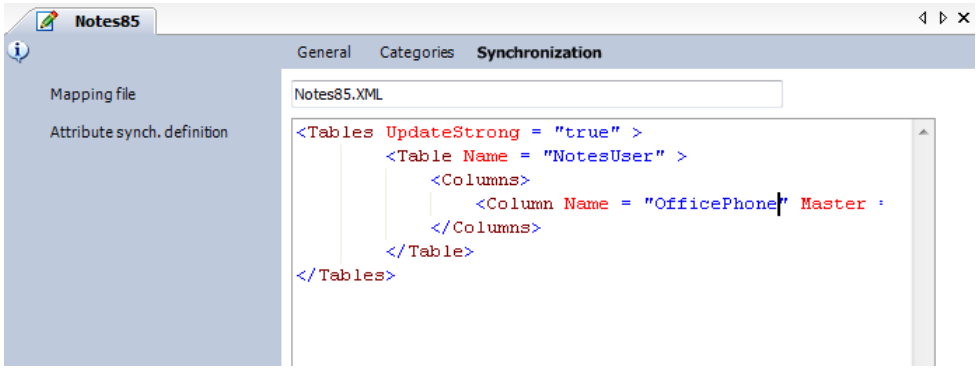
  Identity Manager: data synchronization between the Identity Manager database and the Lotus Notes domain is carried out by the synchronization components from the Identity Manager.
  FIM: data synchronization between the Identity Manager database and the Lotus Notes domain is carried out by the Microsoft Forefront Identity Manager.
  No synchronization: no changes are automatically transfered from the Identity Manager database to the Lotus Notes domain.

  You can only specify the type of synchronization when a new client is added. Once it has been saved, no changes can be made. If you select ”No synchronization“ you can define custom processes to exchange data between the Identity Manager and the Lotus Notes domain.

How to Customize Data Synchronization

At this point, you can make special adjustments for synchronizing the data between the Identity Manager database and Lotus Notes. Since the requirements within a Lotus Notes environment may be different from domain to domain, you can make changes to each Lotus Notes domain individually.

Customizing Data Synchronization



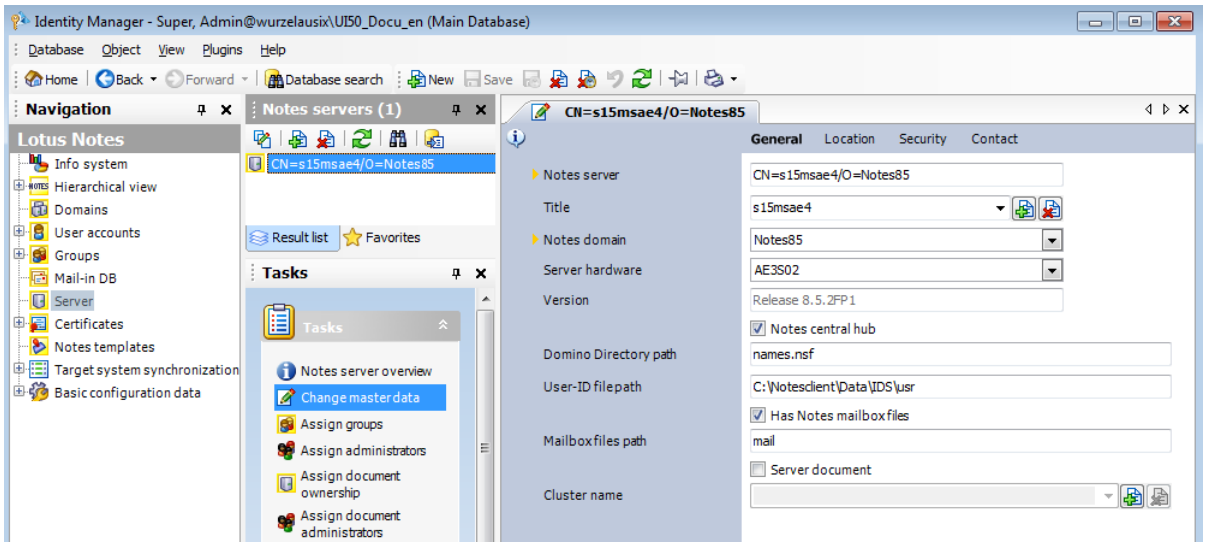
The mapping file contains the templates for mapping target system specific objects, such as user accounts, groups or mail-in databases, between the Identity Manager database and Lotus Notes domains. The evaluation is carried out using target system specific process components. An external mapping file only has to be given if the default mapping for the data should not be used. This external mapping file must exist on the gateway server. If no path is given, the mapping file has to be in the Identity Manager Service install directory on the gateway server. Refer to section Customizing Mapping rules on page 180 for further infomation.

You can specify the master for data synchronization for individual target specific object properties with the attribute synchronization definition. The input is entered in an XML structure. Refer to the section Specifying the Data Master for Object Properties on page 192 for more information.

Declaring the Domino Servers in the Identity Manager Database

The Domino server is set up in the Manager in the category <Lotus Notes>\<Server>.

Setting Up the Domino Servers



The following information about the Domino Server is required in the Identity Manager for synchronization:

- Notes server name
  Enter the common name for the Domino server into the Domino Directory. The common server name is made up of the name that is given when the server is registered and the certificate name, which is used for the server registration.

- Notes domain name

- Server hardware name
  Select the server that is installed on the Domino server. All Identity Manager database servers are offered for selection.

- Label the Domino server as Notes central hub

- Notes address book
  Enter the name of the primary Domino Directory (Names.nsf) in the Domino server.

- User ID file path
  Enter the path that is used to created new user ID's. The user ID files are created on the gateway server.

- Has Notes mailbox files
  With this option you mark the Domino server that can keep mailbox files. These servers are available for selection as mail servers when users are set up.

- Mailbox file path
  Enter the path to the mailbox files on servers that may store them. In the case of Lotus Notes Server Release 6, enter the default path "C:\Lotus\Domino\Data" to the mailbox file repository. Earlier version of Lotus Notes servers use the path "C:\Lotus\Notes\Data" for storing the mailbox files.

This input does not, however, have any meaning for the function of the server as snychronization server.

Testing Domino Server Functional Efficiency

To check whether a Domino Server is functionally efficient, an attempt is made to open it's database "Admin4.nsf". Enable the scheduled task "Lotus Notes checking the current server" to run the test regularly. You can modify this request to suit your requirements with the help of the Schedule Editor in the Designer. Read section Setting Up Scheduled Tasks on page 73 for more information.

Accelerating Synchronisation

Configuration Parameter for Accelerating Synchronization

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\UseUSN	When Notes objects are synchronized, a comparison is carried out using the change date.

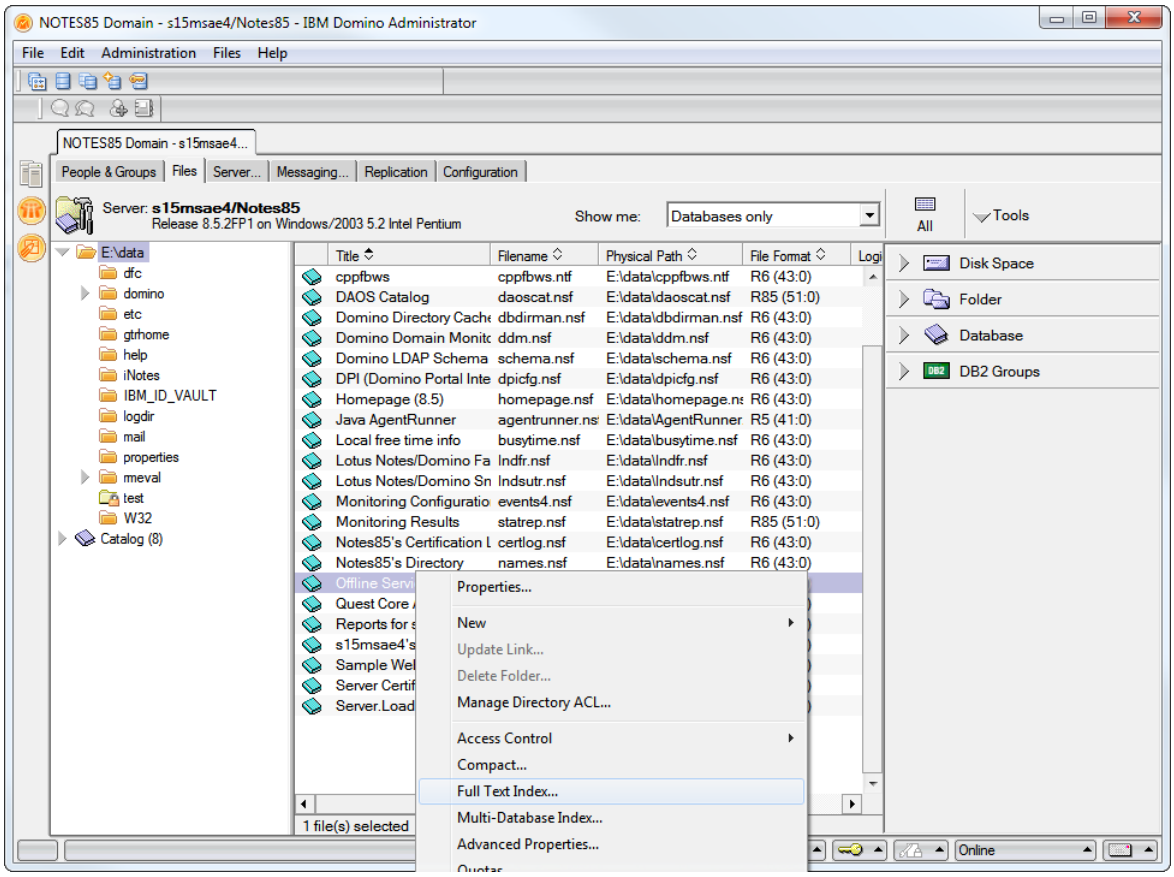
All Lotus Notes documents from one view are loaded during synchronization. You can implement a document filter to speed up the synchronization as this procedure can be very time consuming in certain circumstances.

Each Lotus Notes document has header information where the date of the last change is saved. Each synchronization saves the last change date in the Identity Manager database. The next time a synchronization is run, only those Lotus Notes documents that have been changed since this date are loaded.

In order to read the date information from the Lotus Notes document, you need to set up a full text index on the Domino server for the server address book. The full text index is set up with the Lotus Do-

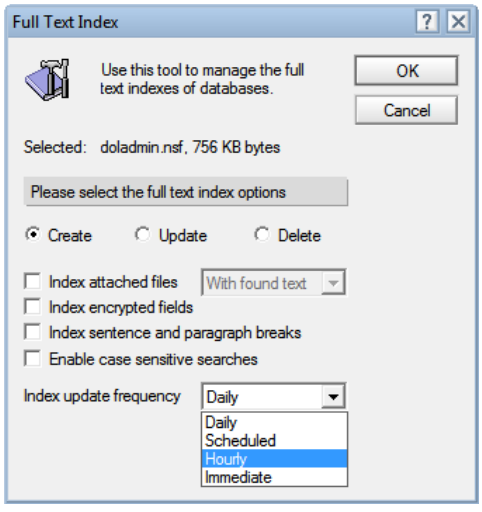
mino Administrator in the 'Files' view. Create a full text index for the server address book from the context menu item <Full Text Index...> and enter the update interval.

Lotus Domino Administrator - Full Text Index Setup 1



In the dialog window that follows, select the "Create" option. Select the update frequency so that the index is either updated in short intervals or as otherwise planned, before synchronization.

Lotus Domino Administrator - Full Text Index Setup 2



For more information on this subject, refer to the Lotus Notes documentation. If the full text index is not updated, all the documents that are not yet included, are not taken into account by synchronization!

Using AdminP Request for Handling Lotus Notes Processes

Lotus Notes contains an asynchronous mechanism for processing various internal tasks. For example, if the name of a user changes, this mechanism ensures that the access control list from the Lotus Notes database is also modified.

The requests are take on by the Lotus Notes server task ”AdminP“ that runs on every Lotus Notes server. This tasks checks at set intervals whether there are new requests pending that require handling. These are placed in the Lotus Notes database ”admin4.nsf“ in the form of request documents and then replicated on every server. After a task has been processed, the executing server creates a response document and if necessary a follow-up request.

AdminP requests are used by certain Identity Manager processes, i.e. for changing parts of a users name, exchanging certificates or when restoring a user ID.

Several factors are involved in determing when these will be processed:

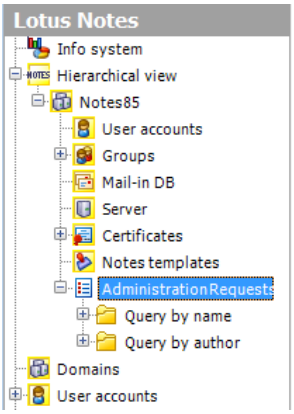
- When was the request replicated on the executing Lotus Notes server?
- How often does the AdminP request run on the executing server?
- Which type of request is it?

Synchronizing AdminP Procedures

In order to create reports about AdminP requests, a regular synchronization of the database ”Admin4.nsf“ is required. For this you use the scheduled task ”LotusNotes loading the AdminP database“. You can modify this request to suit your requirements with the help of the Schedule Editor in the Designer. Read section Setting Up Scheduled Tasks on page 73 for more information.

AdminP request and responses are displayed in the category <Lotus Notes> in the hierarchical list of Lotus Notes domains.

Displaying AdminP Requests



Accelerating Handling of AdminP Requests

Configuration Parameter for using AdminP Requests

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\Accelerate-AdminP	Starts the AdminP queries on server immediately

The AdminP server task starts on its own at certain intervals on different servers. If these intervals are large, it may take some time before a pending request is run. For example, it is preferable for a pending request to be run without delay when an ID is restored, so that the user is able to login as soon as possible.

For this purpose, set the configuration parameter ”TargetSystem\Notes\AccelerateAdminP“. This ensures that, in the case of processes, the command ”tell adminp process interval“ is sent to the Lotus Notes server via remote console. This means that request processing starts immediately, which normally would not be done until the next time the AdminP server task was performed at the regular time.

This function can cause a heavy load on the server if there is a large number of processes. .

Automated Confirmation of AdminP Requests

Cerain AdminP requests have to be confirmed first by the administrator before they can be run. It is possible to confirm them automatically with the Identity Manager. Prerequisite for this is regular synchronization of the Admin4 database.

The confirmation of open requests can be triggered at regular intervals by the scheduled task ”LotusNotes Automatische Bestätigung von AdminP Requests“ (LotusNotes automatic confirmation of AdminP requests). You can modify this request to suit your requirements with the help of the Schedule Editor in the Designer. Read section Setting Up Scheduled Tasks on page 73 for more information.

Confirmation of the following requests has currently been implemented:

- Approve MailfileDeletion
- Approve MovedReplicaDeletion
- Approve ReplicaDeletion

Basic Configuration Data

Target System Manager

You can assign employees in the Identity Manager to every Notes domain that can edit the objects in this domain in the Identity Manager. To do this, assign an application role <Target system manager> in the Notes domain general master data. Assign the employees to this role that are authorized to edit Notes domains in the Identity Manager.

Edit target system managers for Lotus Notes in the Manager in the category <Lotus Notes>\<Basic configuration data>\<Target system managers>\<Lotus Notes> or in the Identity Manager in the cate-

gory <Identity Manager Administration>\<Target systems>\<Lotus Notes>. You can find more detailed information about application roles in section The Identity Manager Roles Model on page 61.

Lotus Notes Certificate

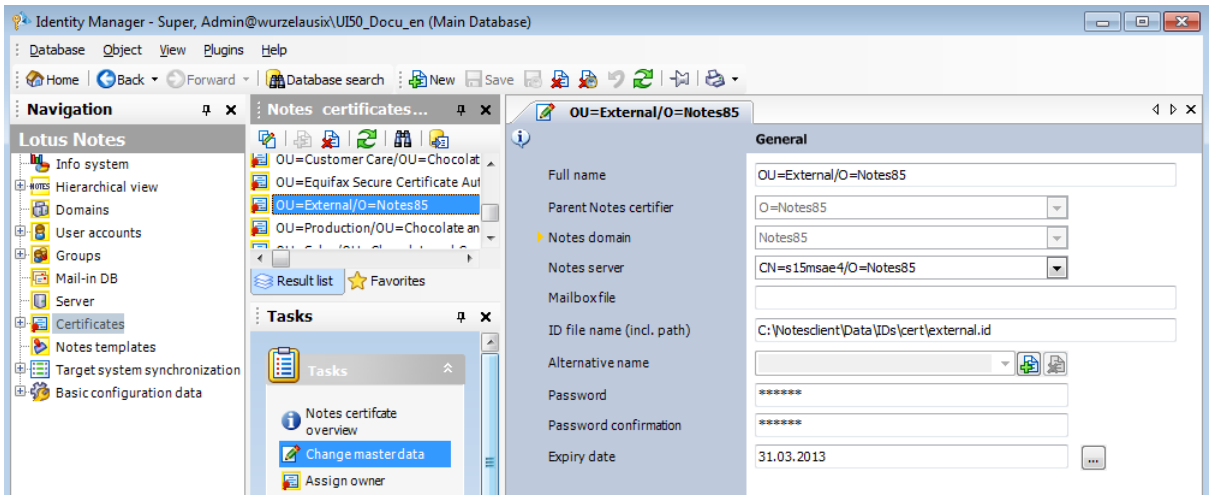
Configuration Parameters for Lotus Notes Certificate

CONFIGURATION PARAMETERS	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\Certifier	Certificate are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesCertifierLocalAdmin	Administrator relation for certificate documents are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesCertifierOwner	Owner relations for certificate document are synchronized between target system environment and database.

Certificates are only read in so that they can be referenced when new users or groups are added. The foreign key relation to user objects allows all user IDs that were added with the Identity Manager, to be restored with the original certificates.

Certificates are displayed in the Manager in the category <Lotus Notes\Certificates>.

Managing Certificates



The following data is stored on the master data form:

- Full name of certifier
- Parent certifier
  Gives the name of certificate issuer.
- The Notes domain
- The Notes server (Domino Server) where the mailboxes are stored and the file path

- Certifier ID file path and name of file
  In the Identity Manager, it is necessary to enter the full ID file path on the gateway server after the initial synchronization for any certificate, that may be used for registering users. This makes it possible to administrate all ID files for the certificate that occurs on the server.

- The alternative certificate name
  For a certifier ID file, you can assign names that can be understood in the user's native language.

- The certifier's ID file password

- The certificate expiry date

Use the forms <Assign owner> and <Assign administrator> to specifiy users and a groups for the certificate, that may edit and manage the document.

Lotus Notes Templates

Configuration Parameter for Lotus Notes Templates

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\DefTemplatePath	Input for default template to adding mail files on a Lotus Notes server

Lotus Notes templates can be managed in the Identity Manager. For example, templates are defined for different Lotus Notes mail client versions to take into account the client version when creating personal address books. Lotus Notes template information is not loaded by synchronization and needs to be manually maintained in the Identity Manager.

Templates are displayed in the category <Lotus Notes>\<Templates>. Enter a name for the template and specify the Notes domain and the template file name.

Lotus Notes templates for creating mail files are determined though the employee's operating data. Use the configuration parameter "TargetSystem\Notes\DefTemplatePath" to specify the default template. This is used when no template can be determined using the IT operating data.

Lotus Notes User Account

Lotus Notes user accounts are employees that use the Notes Client for accessing the Domino server and the database. A set of user specific data has to be generated for certifing new users for Lotus Notes. This data needs to be available to the user for working with Lotus Notes on his or her local PC or in the home directory.

All Lotus Notes user accounts known to the Domino Directory are displayed in the Identity Manager. When a user is added, the user ID file for authentication, the mailbox file and the user's personal address book are added. The mailbox file is created on the given mail server, the ID file and the personal address book are created on the gateway server.

The Identity Manager works with several methods to create user accounts and assign them to employees.

- Employees and user accounts can be manually entered and assigned to each other

- Employees automatically obtain their user accounts over user account resources. If an employee does not have a user account in a Lotus Notes domain, it is created by assigning the user account resource to an employee using the inheritance mechanism integrated into the Identity Manager and subsequently processing a new Lotus Notes user account. This method is described in more detail in section Managing Lotus Notes User Accounts with User Resource Accounts on page 324.

- When a user account is added, an existing employee is automatically assigned and if necessary created. The employee master data is created based on the existing user accounts. This mechanism be used when a new user account is created either by manually adding it or by synchronization. This is, however, not the default method for the Identity Manager. This method is explained in the section Automatic Assignment of Employees to User Accounts on page 40.

The basic mechanisms are dealt with in the chapter Employees and User Accounts on page 25.

Entering Lotus Notes User Account Master Data

Configuration Parameters for Setting Up Lotus Notes User Accounts

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\CreateMailDB	A mail database is created on the mail server when a new Lotus Notes user account is added.
TargetSystem\Notes\IsNorthAmerican	Specifies whether the Notes ID files are compatible with the american(US) and canadian Lotus Notes version.
TargetSystem\Notes\PersonAutoDefault	Depending on this parameter mode, automatic assignment of employees takes place when a user account is added.
TargetSystem\Notes\StoreIDInAddressbook	The ID created for a new Lotus Notes user account is attatched to the user document.
TargetSystem\Notes\SyncObjects\Person	Users are synchronized between target system and the Identity Manager database.
TargetSystem\Notes\TempNetworkPath	Temporary directory where newly created ID files and personal address books are stored.
TargetSystem\Notes\UpdateAddressbook	Entries are created in the main address book when new user IDs are created.

A Lotus Notes user account can be linked to an employee in the Identity Manager. However, Lotus Notes user accounts can also be managed separately from employees, for example to create administrative user accounts.

Lotus Notes user accounts are displayed in the category <Lotus Notes>\<Users>. You can enter the necessary data on the <Change master data> form and if necessary rework it. Please make sure that all compulsory fields are filled.

We recommend using user account resources to set up a Lotus Notes user account for a company employee. If you do use a Lotus Notes user account account resource to set up the user, some of the master data that is described in the following is created using templates. E.g. Lotus Notes server and Lotus Notes user account certificates. Certain employee master data is inherited using employee Lotus Notes user account templates. The range, in this case, is based on the default manage level for the user accounts resource. The templates supplied should be customized as required.

General Master Data for a Lotus Notes User Account

Configuration Parameter for General Data

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\MailBoxAnonym-Pre	Prefix for Lotus Notes user account anonymity.

Enter the general master data for a Lotus Notes user account on the <General> tab. You may assign an employee to a user account. If the user account was created using a user account resource, an employee will already be entered. If you use automatic employee assignment, a associated employee is created and entered into the user account when the user account is saved. If you do not use any of these methods but manually create the user account, you can also assign an employee manually to the user account.

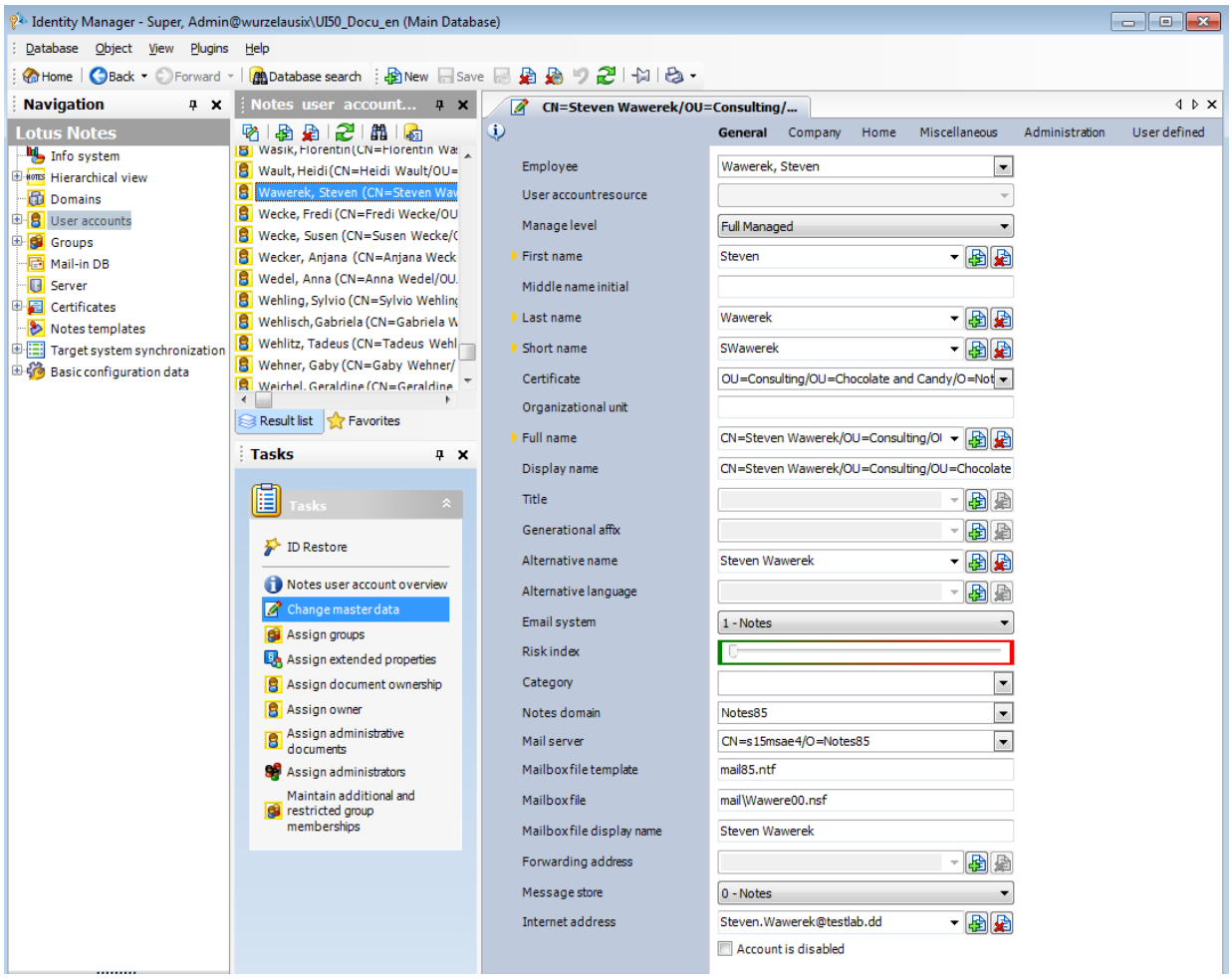
When user account resources are assigned to an employee or a resource to a company structure, an associated user account is created with the integrated inheritance mechanism and the process handling that follows. If the process handling fails because, for example, not all the neccesary IT operating data could be found, you can also create the user account manually and, at the same time, select the user account resource to use. Only the target system user resources are shown in the pop-up menu <User resource account>.

The user account manage level is decided by the range of the employee's properties that are passed on to the user account. The Identity Manager's default installation is configured for the manage levels "Unmanaged" and "Full managed". User accounts with the manage level "Unmanaged" are merely linked to an employee but do not inherit other properties. User account with the manage level "Full managed" inherit defined employee properties. You can define other manage levels depending on the company's requirements.

When a user account resource is assigned to an employee, the default manage level of the user account resource is used to create the user account. Normally, the manage level "Full managed" is used as default. If you create the user account manually or with automatic employee assignment, the manage le-

vel is ”Unmanaged“. You can change the levels after the user account has been saved using the pop-up menu <Manage level>, provided that the Lotus Notes domain has a user account resource.

General Data for a Lotus Notes User Account



You need to enter a name, initials, surname, title and generational affix for a Lotus Notes user account. The short name is automatically made up of the user’s first and last names. If the user’s first name or last name is changed, an additional short name is automatically created.

Select the certificate that should be used for creating the user ID. The certificate is determined from the IT operating data for the employee assigned depending on the manage level of the user account. The full name and display name for the Notes user is detemined by the name data and the certificate. The foreign key relation to user objects allows all user IDs that were added with the Identity Manager, to be restored with the original certificates. The certificate is crucial for managing user accounts through user account resources in making the other Lotus Notes user account properties.

When Lotus Notes user accounts are synchronized from the Lotus Notes environment to the Identity Manager database, the certificate assignment cannot be loaded. If a Lotus Notes user account is initially loaded into the database or if his or her certificate has changed in the environment, you need to enter the certificate assignment into the Identity Manager database afterwards.

In addition, enter an organizational unit for the user.

You can enter an alternative name for a Lotus Notes user account in the users own language. The alternative name must be connected to another user language.

Lotus Notes User Account Account Email System

Configuration Parameter for Creating a Mail File

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\DefTemplatePath	Specifies the default template for adding mail files to the Lotus Notes server.
TargetSystem\Notes\MailFilePath	Gives the directories on the mail server underneath C:\Lotus\Notes, where the Lotus Notes user account mail files are stored.

Selec the email system that the user is going to use on the <General> tab. Depending on which chosen email system, the properties described below are shown for addressing.

There is the following choice:

- Notes
- cc:Mail
- Other
- X.400
- Other Internet Mail
- POP / IMAP
- None
  If no mail system will be used enter "None".

Enter the Lotus Notes user account domain and select the mail server for the email systems "Notes" and "POP/IMAP". All Notes servers that are labeled with the option <Has Notes mailbox files> in the Identity Manager database are available for selection as mail server.

The mail file template determines which client version is used to create the mail file for a user. The data can be determined through the employee's IT operating data. If a template has no been given, the configuration parameter "TargetSystem\Notes\DefTemplatePath" is used to define the default template.

The short name is used to make the mailbox name. The path input and the name of the mailbox is done using a template and can be customized. The user's mailbox is stored in a special directory "Mail" on the given mail server under the specified mailbox path. The directory name is specified by the configuration parameter "TargetSystem\Notes\MailFilePath". Enter an forwarding address if the user does not receive messages given mail server and the given mailbox. This has to include the complete mail address of the user (including domain name).

The viewable area of the mailbox store is given by selecting the message store. Choose from the following:

- Lotus Notes
- Lotus Notes and Internet Mail

- Internet Mail

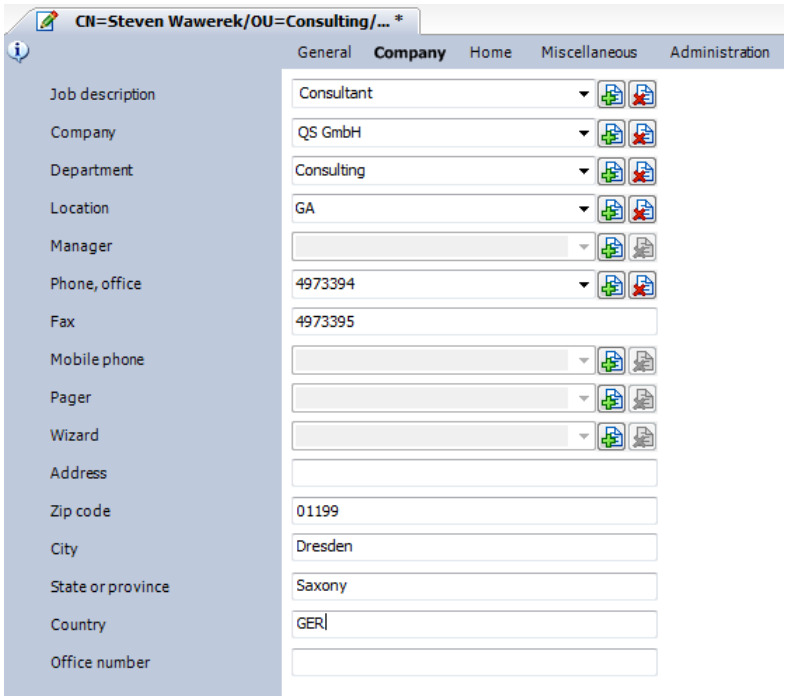
The internet address is used to identitfy the message recipient when a message is received through SMTP in the Lotus Notes environment. Enter the user's full SMTP address. The internet address is created from the employee's default email address depending on the manage level of the user account.

For the email system "cc.Mail", enter the Lotus Notes user account domain, the internet address, the cc.Mail Post Office, the cc.Mail user name and the cc.Mail location. For the email systems "Other" and "Other internet mail" enter the Lotus Notes user account domain, the internet address and a forwarding address to send the user's messages onto. For the email system "X.400" enter the Lotus Notes user account domain, the X.400 server and the X.400 user address.

Lotus Notes User Account Address Data

Enter the address and telephone information for contacting the employee that uses this user account on the <Company> and <Private> tabs. Enter other known data for describing the user in more detail. This data is copied to the master data depending on the manage level of the user account.

Lotus Notes User Account - Address Data



Additional Master Data for a Lotus Notes User Account

Configuration Parameter for additional Master Data

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\ReadMailfileSize	User mailbox parameters are loaded into the database during synchronization.
TargetSystem\Notes\SecurityType	Encryption depth for calculating a Notes ID file.

Enter the additional data for a Lotus Notes user account account on the <Miscellaneous> tab. This data is mainly for the mail file and message forwarding.

The size of the user's mail file is determined by a scheduled task "MailfileGrössen NOTESUser einlesen (Load NOTESUser MailFileSize)" that you can enable and configure in the Schedule Editor. Read the section Setting Up Scheduled Tasks on page 73 for more information. Prerequisite for determining the mail file size is the correct mail server input and the mailbox path.

You can limit the size of the user's mailbox with the option <Max. size [kb]>. Specify a warning threshold above which the user is sent a mail when the value is exceeded.

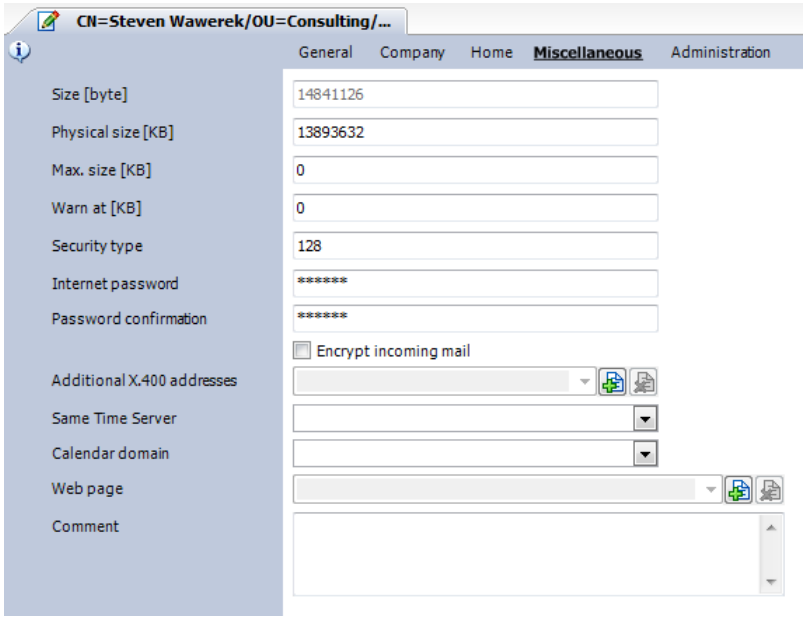
Use the security type to specify the encryption depth to be used when a user ID file is created. The permitted values are defined using the configuration parameter "TargetSystem\Notes\SecurityType". Security types cannot be assigned to user through synchronization.

You also can allocate an internet password to the user. Web users have to use this password for authentication on a Domino web server.

Save any additional information required for passing messages on to the user. Specify whether incoming messages should be encrypted. You can add another email address for the user in X400 format.

Other input is the 'same time server', the calendar domain and the user's website. Enter a same time server for users who use the 'sametime' function from Lotus Notes. Enter a calendar domain for users that use another calendar and time plan function. This input is used to forward user requests for free time on another domain if the message can be received.

Lotus Notes User Account - Miscellaneous



Administrative Data for a Lotus Notes User Account

Configuration Parameter for Password Data

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\Accounts\Initial-Password	Preset password for adding user accounts.
TargetSystem\Notes\Accounts\Initial-RandomPassword	A random generated password is generated when a new user account is added. It must contain at least those character classes that are set in the child configuration parameters.
TargetSystem\Notes\MinPasswordLength	Specifies the minimum password length that is set in all newly calculated Notes ID files.
QER\Person\UseCentralPassword	The employee's central password is automatically mapped to the employee's user account in all permitted target systems.

Specify how the user should be authentified on the server with the password check type. Password check types are:

- Do not check password (0 = dont check)
- Check password (1 = check)
- Disable ID (2 = Lockout ID)

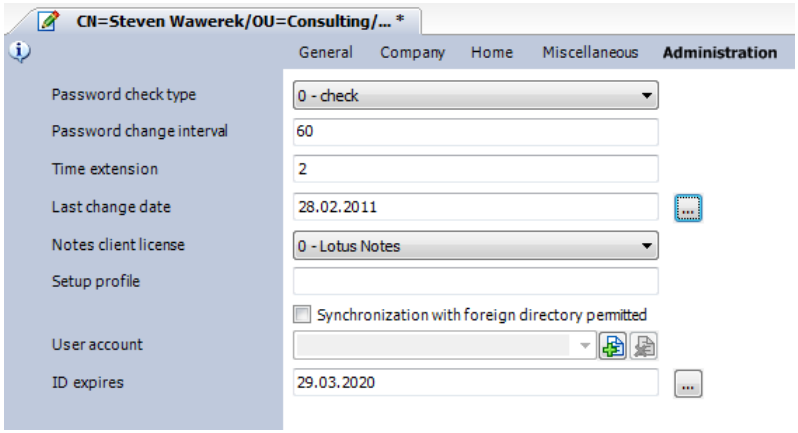
When new user is added the password check type "0 = dont check" is assumed as default. The user with password check type "2 = Lockout ID" cannot log onto any server in the domain that checks passwords (see Lotus Notes Servers on page 335).

In addition, you can specify a time interval for changing the password and set an extension to this. After the password change interval has expired, the user is blocked from accessing servers until the password has been changed. If this does not occur within the given time extension, the user can no longer log onto a server. The date of the last password change is determined automatically and cannot be changed.

When a user is added, you issue them with a password. Once the user has been saved you cannot change the password anymore in the Manager. The corresponding fields are grayed out. You can set an initial password for newly added user accounts with the configuration parameter "TargetSystem\Notes\Accounts\InitialPassword". Use the parameter "TargetSystem\Notes\Accounts\InitialRandomPassword" to specify whether a randomly generated password should be issued to a new user account. The child parameters specify the character sets that the password needs to contain and the email address that the password should be sent to. Depending on the configuration parameter "QER\Per-

son\UseCentralPassword", the employee's main password can be mapped from the user account password.

Lotus Notes User Account - Administration



You can specify a user's client license. The license type determines the range of user access. Possible license types are:

- Lotus Notes Desktop
- Lotus Notes Mail
- Lotus Notes

The license type "Lotus Notes" is assumed as default when a new user is added.

Enter the name of the configuration profile to be used for the user in the input field <Setup profile>. Other administrative input concerns synchronization with foreign systems. If the user name can be synchronized with other systems, set the option <Synchronization with foreign directory permitted>. Enter the user account that is going to be used for synchronizing between Lotus Notes and other system, for example, Active Directory or Windows NT, in the input field <User account>. The user ID expiry date is calculated with a template and displayed in the input field <ID expires>.

The user ID expiry date is calculated from a template and displayed in the field <ID expires>. User ID's that expire in less than 10 days, can be renewed for 2 years by running the scheduled task "LotusNotes ID-Ablaufdaten automatisch verlängern" (Automatically renew Lotus Notes ID expiry date). You can customize this task to meet your requirements and start it with help from the Schedule Editor in the Designer. Read the section Setting Up Scheduled Tasks on page 73 for more information.

Additional Tasks for Managing Lotus Notes User Accounts

After you have entered the user account master data, you can apply different tasks to the it. You can see the most important information about a user account on the overview form. The task view contains different forms with which you can run the following tasks.

Assign Lotus Notes Groups directly to Lotus Notes User Accounts

All Lotus Notes groups are shown on the overview form. Lotus Notes groups can be assigned directly or indirectly. Indirect assignment is carried out by allocating the employee and the Lotus Notes groups to roles. If the employee has a user account, the Lotus Notes groups in the role are inherited by the user acount. To react quickly to special requests, you can assign Lotus Notes groups directly to the user account. To do this you use the for <Assign groups>. See section Assigning Company Resources through Roles on page 78 for more information on group management.

Specify Documents for Processing

Specify the documents that a user can own on the form <Assign document ownership>. Enter the documents the user can administrate on the <Assign administrative documents> form.

Specify Owner and Administrator Relations the User document

Configuration Parameter für Owner/Administrator Relations

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\Notes UserLocalAdmin	User document administrator dependencies (user, groups) are synchronized between target system and the Identity Manager database.
TargetSystem\Notes\SyncObjects\Notes-UserOwner	User document owner dependencies (user, groups) are synchronized between target system and the Identity Manager database.

Assign the users and groups that can edit this user document on the forms <Assign owner> and <Assign administrator>.

Managing Lotus Notes User Accounts with User Resource Accounts

You can automatically create Lotus Notes user accounts for company employees with the help of user account resources. You can set up user account resources for any domain in a Lotus Notes environment. The basic mechanisms are explained in the section Creating User Accounts with User Account Resources on page 37.

Should an employee get a user account through user account resources, he or she must have a central user account and receive the IT operating data over a primary department, location or cost center assignment. Read more in section Handling Employees and User Accounts on page 30.

In the default installation, a check is made to see if a user account already exists in the user account resource domain. If there is no user account, a new user account is created with the user account resource default manage level. If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

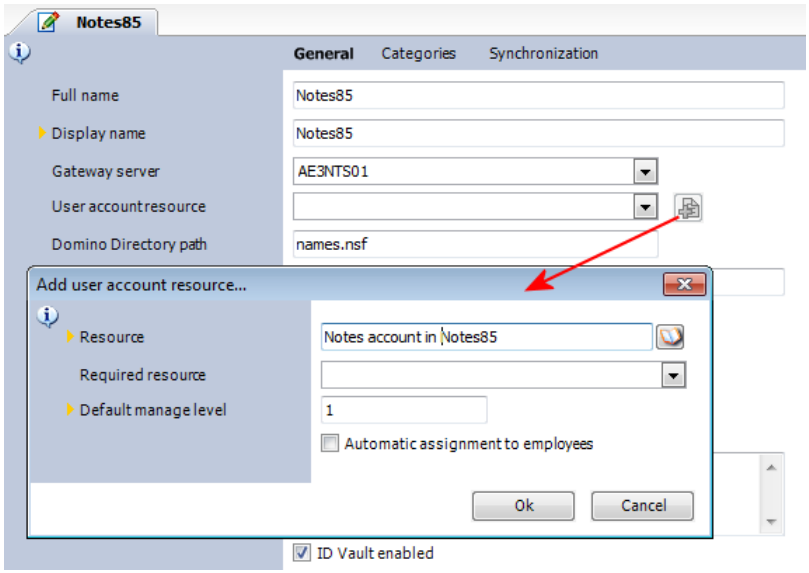
Creating a User Resource Account for a Lotus Notes Domain

Configuration Paramater for User Account Resoures

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\UniqueDefaultManageLevel	When the parameter is set, a different default manage level is expected for each user account resource in the target system (default). If the parameter is not set, each user account resource in the target system may have the same default manage level.

You can set up a user account resource for a Lotus Notes domain in the category <Lotus Notes>\<Domains>. Enter the data for the new user account resource on the domain's master data form by clicking the button next to the corresponding field.

Setting up a User Account Resource for a Lotus Notes Domain

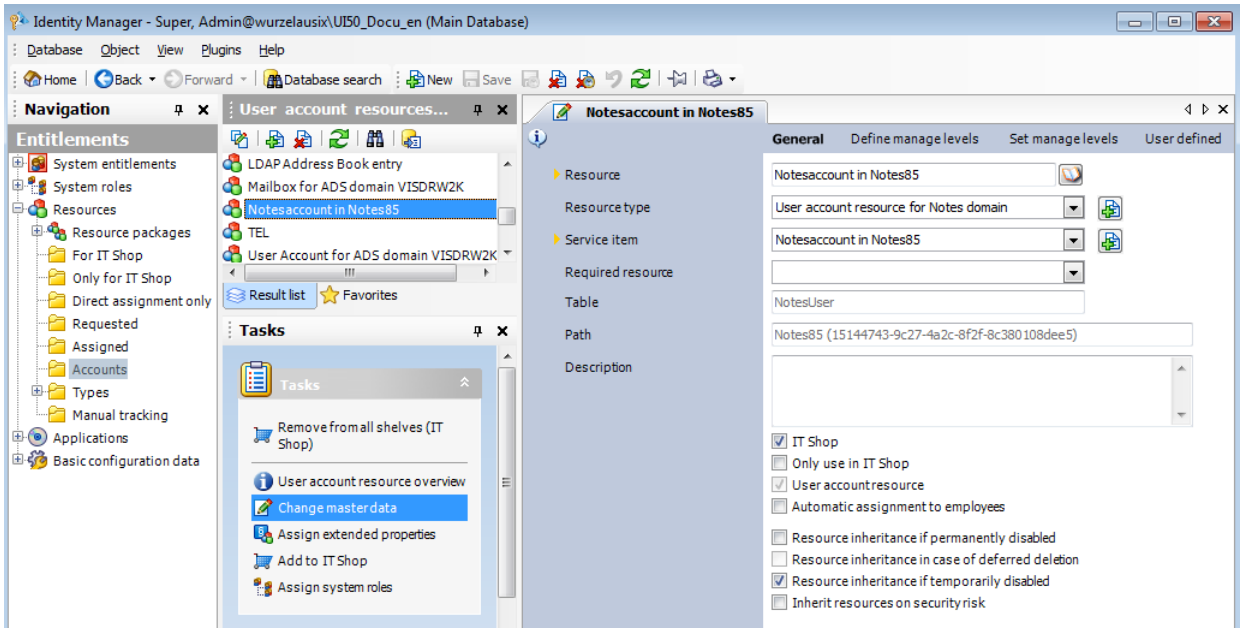


Enter the following data for the user account resources:

- Resource identifier
- Default manage level
  Specify the default manage level that will be used when a new user account is added using this user account resource with the option <Default level>. To create user accounts in the Identity Manager default installation with a manage level "Full Managed" enter the value "1" here. User accounts with an manage level "Unmanaged" are created if the default level is "0".
- Assumed resource
  This field defines a dependency between user account resources. Leave this field empty for Window NT domains.
- Automatic assignment to employees
  Label the user account resource with this option when it should be automatically assigned to all internal employees. The user account is assigned to every employee that is not marked as external on saving. The moment a new employee is added, they also are assigned this user account.The assignment is computed by the DBScheduler.

A new user account resource is created when the data is saved. You can subsequently edit the other data for this user account resource in the category <Resources & Groups>\<Resources> in the filter <Accounts>.

Reworking the User Account Resources



Additional data for user account resources is:

- A resource type.
  Resources should obtain a resource type. This resource type defines future post-processing steps for resource requests or resource assignments.

- The base table in which the user is displayed.
  This input is preset with the value ”NotesUser“ when the user account resource is assigned to a Lotus Notes domain and cannot be changed.

- The domain path used by the user account resources
  This input is preset with the NetBIOS name of the Lotus Notes domain when the user account resource is assigned to a Lotus Notes domain and cannot be changed.

- Service item
  Assign a <service item> to the user account resource or add a new one. This way the user account resource can be booked internally.

- Data for use in IT Shop
  Mark a user account resource with the option <IT Shop> if it is going to be requestable in the IT Shop. These user account resources can be requested by the employees over a web front-end and distributed with a defined approval policy. The user account resource can still, however, be assigned directly to an employee and non-IT Shop roles. In order to avoid direct assignment, activate the option <Only use in IT Shop>. In this case user account resources can only be requested through the IT Shop.

- Data when a currently disabled employee inherits the resource
  You define the inheritance behavior of the user account resource yourself. The inheritance options of the previous resources are overwritten. This resource inheritance behavior may be desired in order to, for example, ensure that all required permissions are immediately reinstated for an employee that is reactivated at a later date. The user account resource options <Resource inheritance if permanently disabled>, <Resource inheritance if temporarily disab-

led> and <Resource inheritance if security risk> are available to map the inheritance behavior. If the user account resource is not passed on when an employee is disabled, the connected employee user account, that was created by assigning this resource, is deleted.

Specifying Rules for Handling Lotus Notes User Accounts

You can specify the manage level for a user account resource for handling Lotus Notes user accounts. The user account manage level determines the scope of the properties that a Lotus Notes domain user inherits from an employee.

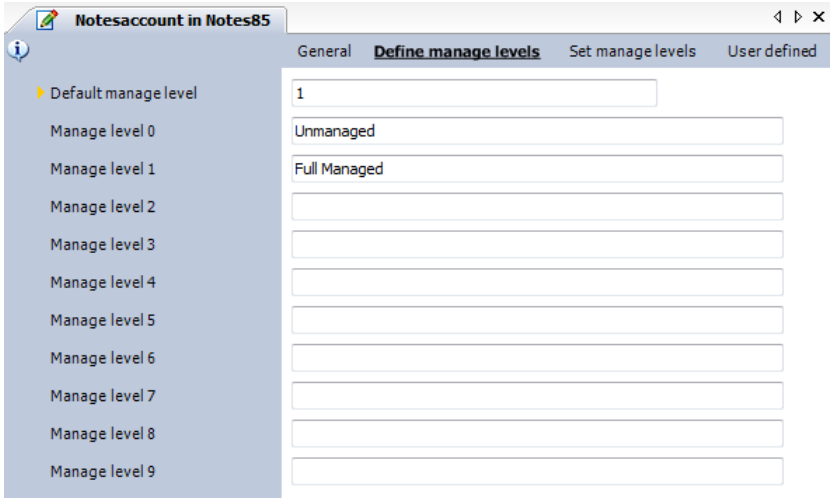
Therefore, an amployee can, for example, have several user accounts in a Lotus Notes domain::

- Default user account that inherits all properties through the employee
- Administrator user account that although linked to the employee, should not inherit any properties.

The Identity Manager delivers a configuration for the manage level ”Unmanaged“ and the manage level ”Full managed“. These manage levels are taken into account in the value templates. User accounts with an manage level of ”Unmanaged“ inherit defined properties from the assigned employee. You can define other manage levels depending on your requirements. Then you need to extend your templates to include the methods for the additional manage levels.

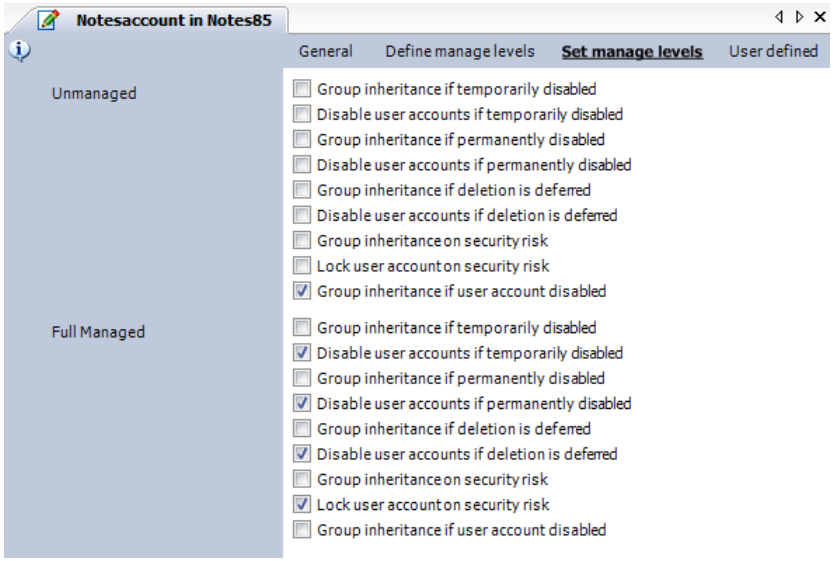
Use the default level to specify the default manage level when new user accounts are added using this user account resource. If more Lotus Notes domains should be managed using user account resources, you have to create a separate user account resource per domain. In the default installation each target system user resource is expected to have a different default manage level. However, the Identity Manager allows several user account resources with the same default manage level to be used. The desired behavior can be controlled with the configuration parameter ”TargetSystem\Notes\UniqueDefaultManageLevel“. There is an example in section Creating User Accounts with User Account Resources on page 37 which explains this in more detail.

Manage Levels for a Lotus Notes Domain User Account Resource



For each manage level, you need to specify the effects of temporary or permanent disabling and deletion of an employee on his or hers user accounts and group memberships..

Editing User Account Resource Manage Levels


Notesaccount in Notes85
General
Define manage levels
Set manage levels
User defined
Unmanaged
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled
Full Managed
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled

The employee's user account can be locked when he or she is disabled or deleted so that permissions are immediately withdrawn. If an employee is re-enabled at a later date, the user accounts can also be reactivated. This behavior is controlled by the properties:

- Disable user accounts if permanently disabled
- Disable user accounts if temporarily disabled
- Disable user accounts if deletion is delayed
- Disable user accounts if security is at risk

Group membership inheritance can be defined for a user account resource for an area of a target system. Inheritance may be discontinued if the employee's user account is locked and therefore may not become a member in a global group. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted! This behavior is controlled by the properties:

- Group inheritance if permanently disabled
- Group inheritance if temporarily disabled
- Group inheritance if deletion is delayed
- Group inheritance if security is at risk

You can find further information in the section Handling Disabling and Deletion of Employees and User Accounts on page 44.

Restoring User IDs

ID restore is an Identity Manager mechanism that can be used when a user has forgotten his password or the ID file itself has been lost. Restoring the ID is started using the task "Restore ID" in the Manager.

The following information is required to run an ID restore:

- An ID file that is initially imported into the database including the associated password.
- The certifier that the initial ID was created with
- a copy of the initially or added user document in the gateway server's 'archiv.nsf"
- The GUID of the document copy in the "archiv.nsf"

This data is automatically generated and saved for the users, that were added in the Identity Manager. An one-off custom import of the files mentioned above has to run for all other user accounts.

The ID restore process executes the following steps:

- Deletes the current user documents from the Domino directory
- Copies the initial user documents from the "archiv.nsf" into the Domino directory
- Exports the inititally saved ID files to the gateway server
- Starts the AdminP request to track the changes made to the original ID up until now. This includes changes to the components of the user's name, changes to the ID expiry date and exchanging certifiers.
- Updates the restored user documents with known values

After the restore has finished, the ID file and the initial password must be supplied to the user. This process should be implemented to suit customer requirements.

Locking and Unlocking Lotus Notes User Accounts

Configuration Parameter for Locking/Unlocking Lotus Notes User Accounts

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\MailBoxAnonymPre	Prefix for Lotus Notes user account anonymity.

A user is considered to be locked in a Lotus Notes environment if it is no longer possible for her to log onto a Lotus Notes server in the domain. Access to her mail database is lost by this. Access to a Lotus Notes server can be prevented if the Lotus Notes user account has the permissions type "Not access server" on the corresponding server document. This is very complicated in environments with several servers because the user to be locked has to entered into said field on every one of the server documents.

For this reason, lock groups are used. Each lock group initially gets the permissions type "Not access server" for each server document. A user that is going to be locked becomes a member of the lock group and therefore is automatically prevented from accessing the domain servers. You can find more information about the concept of lock groups in section Lock Groups in the Identity Manager on page 332.

Set the option <Account disabled> if you want to lock a Lotus Notes user account. After this the Lotus Notes user account is anonymus and is not shown in address books. Access to Lotus Notes servers is removed. The configuration parameter TargetSystem\Notes\MailBoxAnonymPre is checked when the user is made anonymus. In order to restore access to the user at a later date, remove the option <Account disabled>. Anonymity is then removed and the user is deleted from the lock group.

Deleting Lotus Notes User Accounts

Effective Configuration Parameters when Deleting User Accounts

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\Accounts\DeleteByAdminP	User documents are deleted using a Note AdminP process.
User\DeleteDelay	Delay execution of a user account deletion.

You can delete a user account from the result list or the menu bar. After confirming the deletion prompt, the user account is marked for deletion. Due to this the Lotus Notes user account is initially locked (see Locking and Unlocking Lotus Notes User Accounts on page 329). Depending on how the configuration parameter ”User\DeleteDelay“ is set, the Lotus Notes user account is deleted from the address booksand the Identity Manager database. During this time, there is the option to retrieve the account over the context menu item ”Undo delete“ and to reset the status to ”changed“.

Lotus Notes Groups

Configuration Parametersfor Setting Up Lotus Notes Groups

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\Group	Groups are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesGroupListOwner	Group document owner relations are synchronized between target system environmen and database.
TargetSystem\Notes\SyncObjects\NotesGroupLocalAdmin	Group document administrator relations are synchronized between target system environmen and database.
TargetSystem\Notes\SyncObjects\NotesGroupMembers	Group memeberships are synchronized between target system environmen and database.

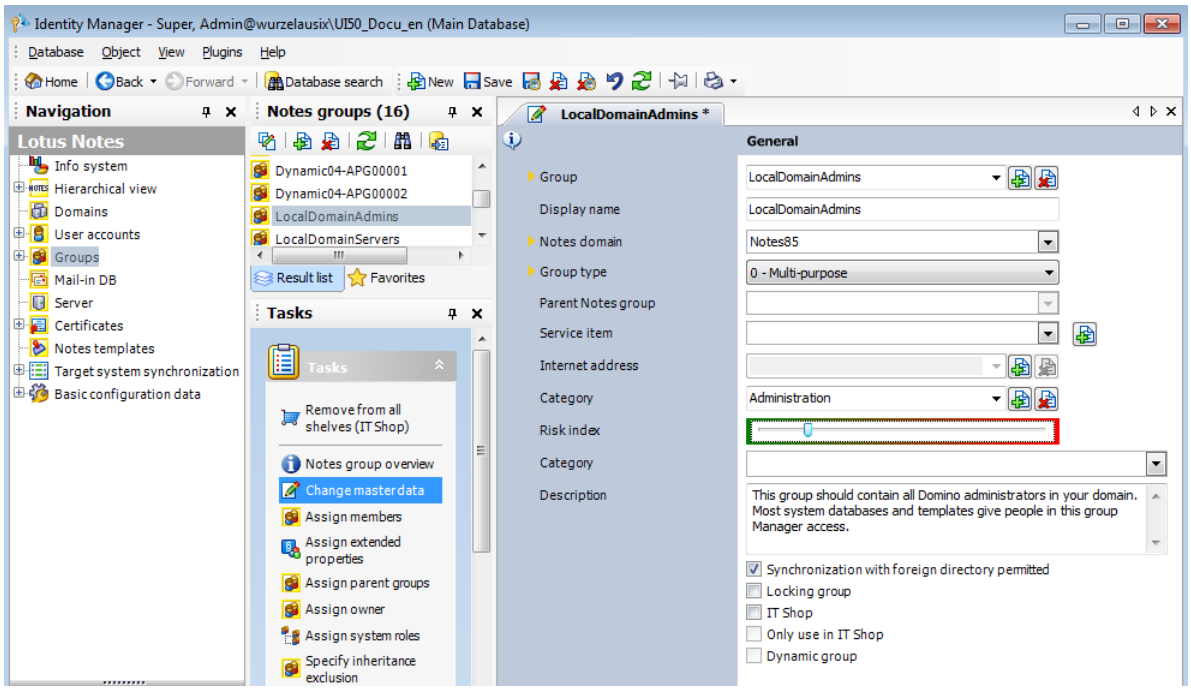
Users, mail-in databases, groups and servers can be grouped together into Lotus Notes groups. Lotus Notes divides groups into different group types. The groups type specifies the group’s intended purpose and whether the group is visible in the Domino Directory.

Applicable groups are:

- Multi-purpose
- Mail only
- ACL only
- Deny List only

The Manager gives you the option to set up a new group or to edit already existing groups. Notes groups are displayed in the Manager in the category <Lotus Notes>\<Groups>

Lotus Notes Groups



When you add a new group, fill in the following fields:

- Group
  Enter the group name that will be used as display name.

- Notes Domain

- Group type
  Select the group type depending on the group's function.

- Category
  Use this field to categorize the group further.

- Internet address
  Enter the group's internet address.

- Synchronization with foreign directory permitted
  If this option is activate, data can be forwarded to foreign directories over this group.

- Lock group
  For more information read section Lock Groups in the Identity Manager on page 332.

- Group description

- IT Shop and service item
  Mark a group with the option <IT Shop> if it is going to be requestable in the IT Shop. These groups can be requested by the employees over a web front-end and distributed with a defined approval policy. The group can still, however, be assigned directly to an employee and non-IT Shop roles. In order to avoid direct assignment, activate the option <Only use in IT

Shop>. In this case, user account resources can only be requested through the IT Shop. To use a group within the IT Shop, assign the group a service item or add a new one. Then the group can be internally booked.

Lock Groups in the Identity Manager

Configuration Parameter for Setting Up Lock Groups

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\DenyAccess-Groups	Lock groups are used when a Lotus Notes user account is disabled.
TargetSystem\Notes\DenyAccess-Groups\Memberlimit	This configuration parameter contains the maximum number of memebers per Deny Access Group. When this limit is reached, another Deny Access Group is created automatically
TargetSystem\Notes\DenyAccess-Groups\Prefix	This configuration paramter contains the prefix used for formating the name of a Deny Access Group.

Immediately after a Lotus Notes user account has been locked, a lock group is found for the user to become a member of. If a lock group of the right type is not found, Identity Manager Service creates a new lock group with the permission type ”Not access server“ and automatically stores it on each Lotus Notes server. The group name is made up of a prefix and an incremental index. Furthermore, these groups are labeled with the option <Lock group>.

Example:

```
<Prefix><Index>
viDenyAccess0001
```

The prefix for the lock group created by the Identity Manager, is defined by the configuration parameter ”TargetSystem\Notes\DenyAccessGroups\Prefix“. It is also possible to define the maximum number of users in a lock group. This is necessary in an environment with a large number of user, to prevent the maximum number of users in one group being exceeded. The configuration parameter ”TargetSystem\Notes\DenyAccessGroups\Memberlimit“ is supplied for this purpose. If this limit is reached, a new lock group is added on all domain servers with an index value incremented by ’1’ and also with the permissions type ”Not access server“.

The script ”VI_Notes_GetOrCreateRestrictGroup“ is responsible for finding and adding lock groups. If lock groups already exist in the Lotus Notes environment, these are dealt with as normal groups. If these groups should also be used for the lock process using the Identity Manager, you have to customize the script accordingly. Set the option <Lock group> for these groups.

Additional Tasks for Managing Lotus Notes Groups

After you have entered the group master data, you can apply different tasks to the Lotus Notes groups. You can see the most important information about a group on the overview form. The task view contains different forms with which you can run the following tasks.

Assign Lotus Notes Groups to Company Structures

It is possible for user accounts to inherit these groups if Lotus Notes groups are assigned to individual company structures. Lotus Notes groups are added to departments, cost centers, locations or business roles. If an employee is added to one of these company structures and this employee has Lotus Notes user account accounts where the <Groups can be inherited> option set, then these accounts become

members of the Lotus Notes group. You can find further information in the section Assigning Company Resources through Roles on page 78.

Inheritance processes are calculated by the DBScheduler. Group inheritance is described in the section How Lotus Notes User Accounts Inherit Lotus Notes Groups on page 294 in the Configuration Manual.

Add Lotus Notes Groups to the IT Shop

When Lotus Notes groups are assigned to an IT Shop shelf the groups can be requested from the shop's customers. To ensure the group is requestable there are further prerequisites need to be guaranteed. There is more information about this in the section Requestable Products on page 33. To remove a Lotus Notes group from the IT Shop, use the task <Remove from all shelves (IT Shop)>.

Add User Accounts, Mail-in Databases, Groups and Notes Server directly to Lotus Notes Groups

Use the form <Assign members> to directly assign Lotus Notes groups directly to Lotus Notes user accounts, servers, mail-in databases and other Lotus Notes groups.

Specify Dependencies between Lotus Notes Groups

Use the form <Specify inheritance exclusion> to define dependencies between Lotus Notes groups. By defining dependencies between the groups, the number of resulting memberships of Lotus Notes user accounts is reduced in the Lotus Notes groups. Read more in section Inheritance Exclusion on page 80.

Assign Extended Properties to Lotus Notes Groups

Extended properties are meta objects for which there is no direct mapping, such as accounting codes, controlling areas or cost center areas, in the Identity Manager data model. These extended properties are used to check rule conformity. For more information see section Setting Up Extended Properties on page 424.

Specify Documents for Processing

Use the formular <Assign document owner> to specify the documents that the group will act as owner for. Use the form <Assign administrative documents> to specify which documents the group may administer.

Specify Owner and Administrator Relations for the User Document

Configuration Parameter for Owner/Administrator Relations

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\Notes UserLocalAdmin	User document administrator dependencies (user, groups) are synchronized between target system and the Identity Manager database.
TargetSystem\Notes\SyncObjects\Notes-UserOwner	User document owner dependencies (user, groups) are synchronized between target system and the Identity Manager database.

Assign the users and groups that can edit this user document on the forms <Assign owner> and <Assign administrator>.

Deleting Lotus Notes Groups

You can delete a group from the result list or using the menu bar. After confirming the prompt the group is marked for deletion and subsequently deleted from the database by Identity Manager Service.

Mail-In Databases

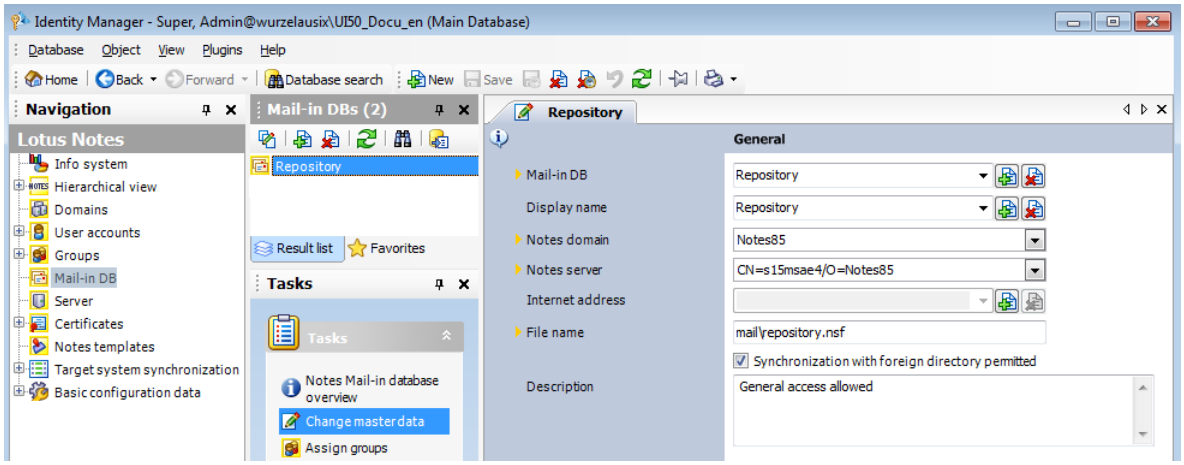
Effective Configuration Parameters

CONFIGURATION PARAMETER	EFFECTIVE WHEN SET
TargetSystem\Notes\SyncObjects\Database	Mail-in databases are synchronized between target system and the Identity Manager database.
TargetSystem\Notes\SyncObjects\NotesMailInDBLocalAdmin	Mail-in database document administrator dependencies (user, groups) are synchronized between target system and the Identity Manager database.
TargetSystem\Notes\SyncObjects\NotesMailInDBOwner	Mail-in database document owner dependencies (user, groups) are synchronized between target system and the Identity Manager database.

Lotus Notes user accounts can send messages between each other or to a commonly used mail-in database. Users can access this mail-in database through the allocation of permissions. When a mail-in database is added using the Identity Manager, a mailbox is created on the given mail server.

Mail-in databases are displayed in the category <Lotus Notes>\<Mail-in DB>.

Lotus Notes Mail-In Database



In order to set up a mail-in database, the following data is required:

- Mail-in database name
  The name of the mail-in database is used as display name.
- Lotus Notes domain name
- Domino Server, where the mail-in database should reside
- Database file name
- Option for allowing synchronization with foreign directory

After setting up the master data for a mail-in database you can:

- Add the mail-in database to Lotus Notes Groups
- Assign the owner/administrator relations for the current employee document
  Assign the users and groups that may edit this mail-in database's document using the forms <Assign owner> and <Assign administrator>.

Lotus Notes Servers

Configuration Parametersfor Setting Up Lotus Notes Servers

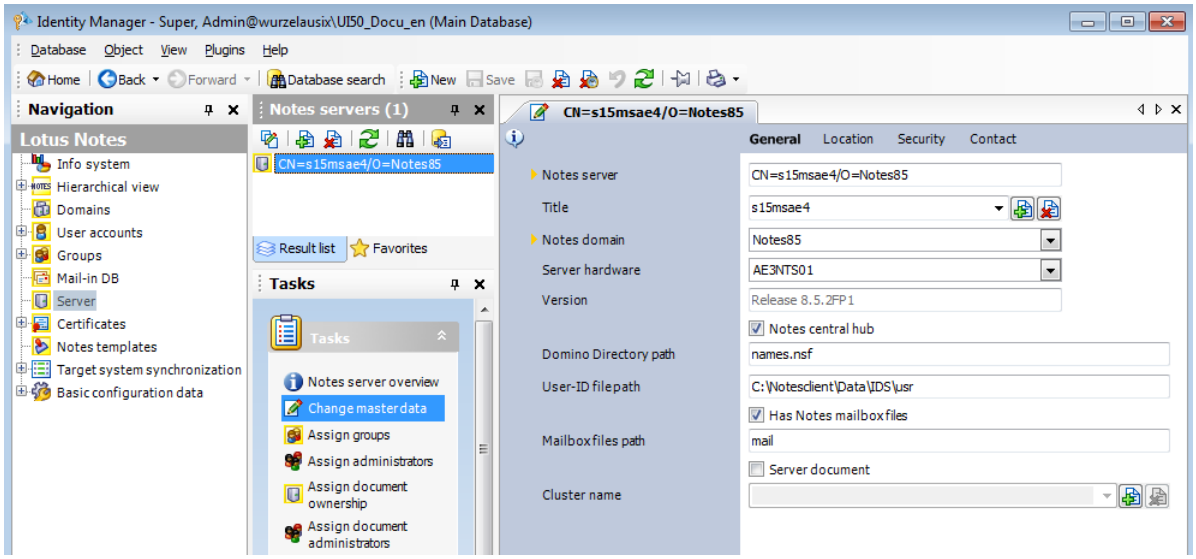
CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\NotesServerLocalAdmin	Server document administrator relations are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerOwner	Server document owner relations are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\Server	Servers are synchronized between target system environment and database.

The Identity Manager displays all known Lotus Notes servers in the primary Domino Directory. If a new server is set up in the Lotus Notes environment, it is entered into the Domino Directory during installation. Server are only loaded by synchronization so that they can be referenced when new users or groups are added.

At this point, the Lotus Notes server properties that are displayed in the Manager will be discussed. Lotus Notes servers are managed in the Manager in the category <Lotus Notes>\<Server>

General Master Data for Lotus Notes Servers

Notes Server Administration



Enter the required data for a Lotus Notes server on the form <Change Master data>.

The following information is found on tab <General>:

- Notes server name
  This shows the hierarchical name of the Domino server in the Domino Directory. The server's hierarchical name is made up from the name given when the server is registered and the name of the certificate that is used when the server is registered.
  Example:

  ```
  CN=Domino01/O=Quest/C=DE
  ```

- Notes Server title
  The title corresponds to the server's short identifier and is used for displaying in the address book.

- Notes domain name

- Server hardware name
  Select the server that the Domino server is installed on. All Identity Manager database servers are available for selection.

- Label the server as Notes central hub
  The option <Notes central hub> is necessary for synchronizing the Identity Manager and the Lotus Notes environment. It should only be set for the Domino server that take parts in synchronization.

- Version
  The version is read from the Notes server ServerBuildNumber during synchronization.

- Notes Address book
  The name given is the name of the primary Domino Directory (Names.nsf) on the Domino server relative to the directory "C:\Lotus\Domino\Data".

- User ID file path
  Enter the path that is used to created new user ID's. The user ID files are created on the gateway server.

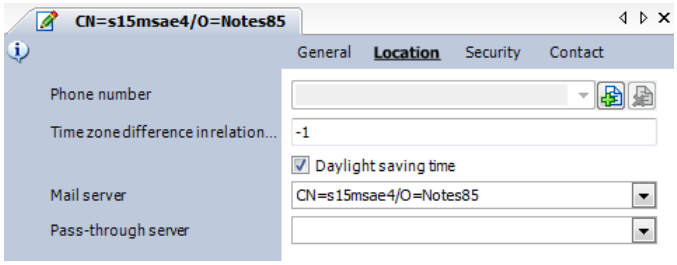
- Has Notes mailbox files
  With this option, you mark the Domino server that can keep mailbox files. These servers are available for selection as mail servers when users are set up.

- Mailbox file path
  Enter the path to the mailbox files on servers that may store them. In the case of Lotus Notes Server Release 6, enter the default path "C:\Lotus\Domino\Data" to the mailbox file repository. Earlier versions of Lotus Notes servers use the path "C:\Lotus\Notes\Data" for storing the mailbox files.

- Cluster name
  The Cluster name is entered here for server that are part of a cluster.

Location Data for Lotus Notes Servers

Location Data for a Lotus Notes Servers



The following data is shown on the <Location> tab:

- Server telephone number
  If the server can take calls over a modem, enter the number here.

- Time zone and daylight saving data at the servers location

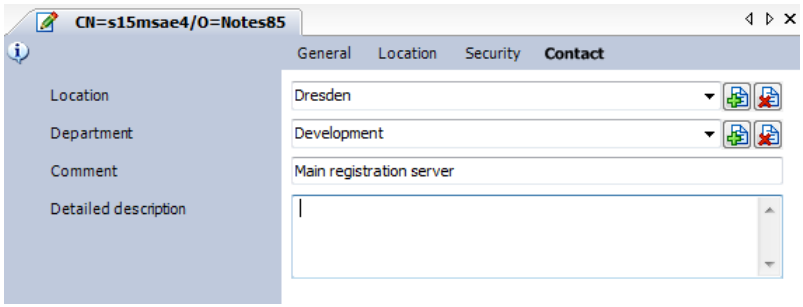
The following fields are relevant when a Lotus Notes client share server data folders with others:

- Mail server
  Select the Notes client mail server that shares the server's data folder with others.

- Pass-through server
  Select the default pass-through server that shares the server's data folder with others..

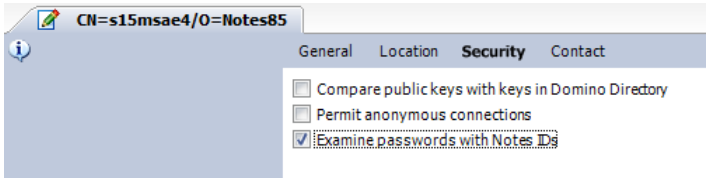
Location information is added on the <Contact> tab. Use these fields to describe the server in more detail.

Contact data for a Lotus Notes Server



Security Settings for Lotus Notes Servers

Security Settings for a Lotus Notes Server



The following security options are displayed on the <Security> tab:

- Compare public keys with keys in Domino Directory
  If this option is set, the server converts a user's public key to a public key in the user's employee document in the domain directory. If these keys do not match, the user may not be able to login on the server.

- Permit anonymous connections
  If this option is enabled, you allow users unauthenticated access.

- Examine passwords with Notes IDs
  If this option is set, the server tests the user ID file password against the password in the employee document to see if it matches. This takes place during authentication.

Server Permissions Settings

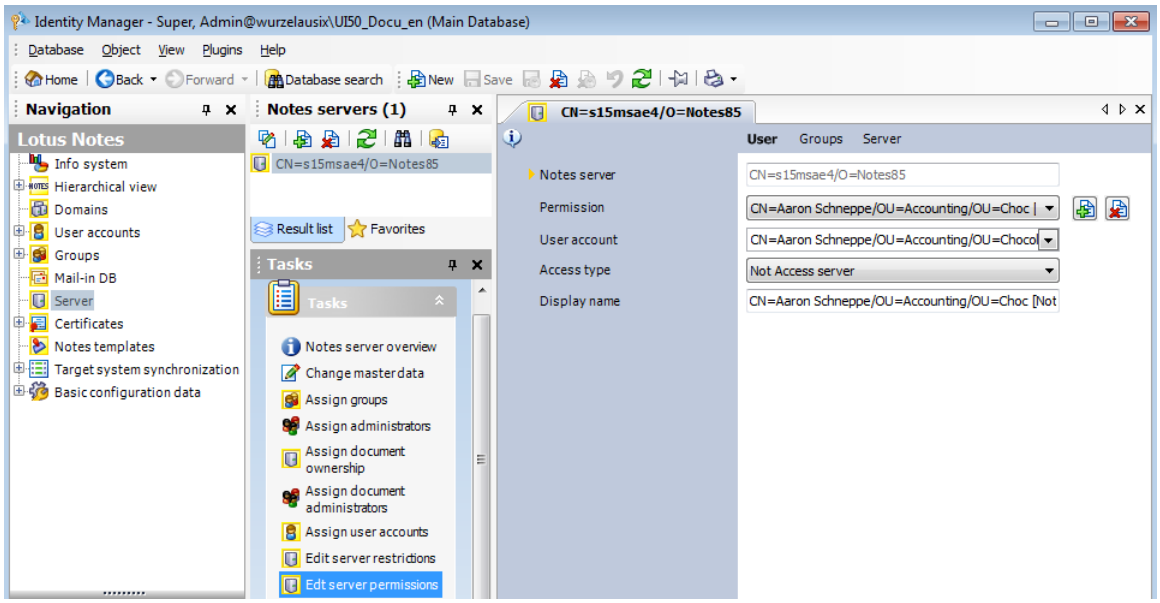
Configuration Parameters for Server Permissions

CONFIGURATION PARAMETERS	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\NotesServerAllowAccess	Server permissions of type "Access Server" are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerBrowserAdminAccess	Server permissions of type "Administer Server from Browser" are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerCreateAccess	Server permissions of type "Create new Databases" are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerDenyAccess	Server permissions of type "Not Access Server " are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerPTAccess	Server permissions of type "PassThruAccess " are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerPTCallers	Server permissions of type "Cause calling" are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerPTClients	Server permissions of type "Route thru" are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerPTTargets	Server permissions of type "Destinations allowed " are synchronized between target system environment and database.

There are several access lists defined in the server document that specify who has access to the server and for what reason. Use the <Edit server permissions> form to define access permissions on the server. Add new access permissions using the insert button on the form. This makes the other fields on the

form editable. Select the user (group, server) that the permissions should apply to and add the permissions type. The display name and the permissions are set when you save.

Specifiying Server Permissions



Permissions types are:

- Access Server
  If no users or groups are given, everyone has server access. If a user or a group is given, then access is restricted to these objects.

- Not Access Server
  Users and groups that are given here may not access the server. This permissions type overrules the type ”Access Server“.

- Create new Databases
  The listed users and groups can create new servers on the database. If no users or groups are given, everyone is permitted to create new databases.

- Create replica Databases
  Only the given users and groups can created database replicas on the server. If no user or groups are given, nobody is allowed to create replicas.

- Administer Server from Browser
  The given users and groups can use the Domino web administrator to manage the server over a web browser. If no users or groups are given, nobody is permitted.

- PassThruAccess
  The given users and group can access the server as pass-through server. If no users or groups are given, the server is not available as pass-through server.

- Route thru
  The given users and groups can connect with other servers using this server. If no users or groups are given, the server is not available as a pass-through server.

- Cause calling
  The given users and groups can connect to other server by call using this pass-through server. If no users or groups are given, the server is not available as pass-through server.

- Destinations allowed
  The given servers can be reached from this pass-through server. If no server is given, all servers can act as targets.

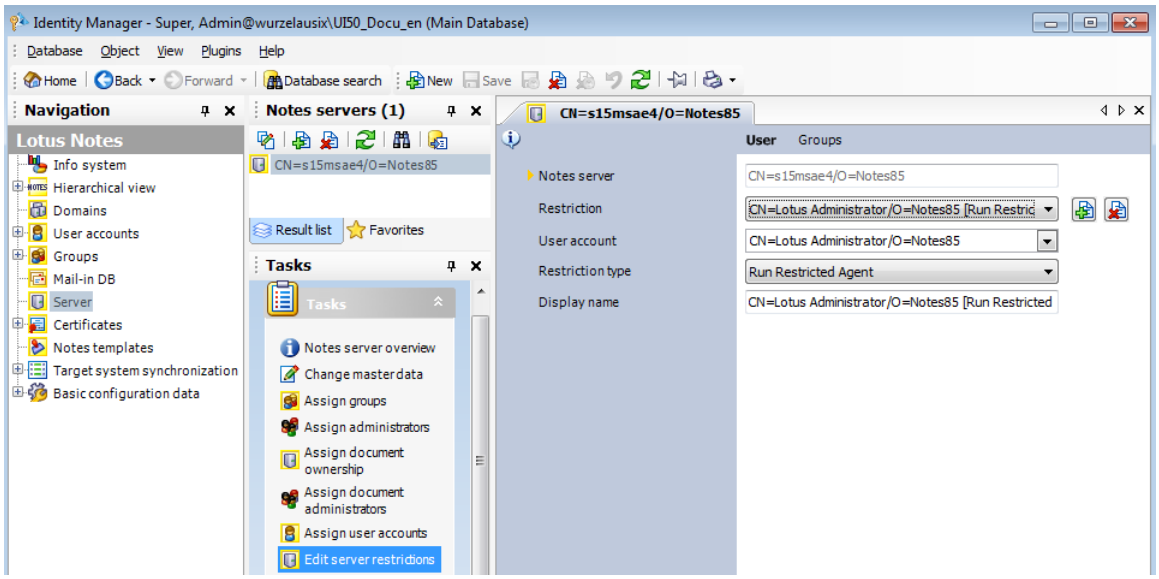
Server Restriction Settings

Configuration Parameter for Server Restrictions

CONFIGURATION PARAMETERS	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\NotesServerPrivateList	Server permissions of type "Run Personal Agent" are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerRestrictedList	Server restrictions of type "Run Restricted Agent" are synchronized between target system environment and database.
TargetSystem\Notes\SyncObjects\NotesServerUnRestrictedList	Server restrictions of type "un Unrestricted Agent" are synchronized between target system environment and database.

Specify which agents the users and groups can use on the form <Edit server restrictions>. Add new restrictions with the insert button on the form. This makes the other fields editable. Select a user (group) that the restriction applies to and set the restriction type. The display name and the restriction are set when you save.

Specifying the Server Restrictions



The restrictions are:

- Run Personal Agent
  Users and groups may execute personal agents. If no users or groups are specfied, everyone can run personal agents.

- Run Restricted Agent
  Users and groups can execute their own LotusScript/Java agents. If no users or groups are given, no one apart from those given under "Run Unrestricted Agent" can run these agents.

- Run Unrestricted Agent
  Users and groups can execute all LotusScript/Java agents. If no users or groups are given, nobody can run these agents.

Additional Tasks for Managing Lotus Notes Servers

After you have enter the server master data, you can apply different tasks to the Lotus Notes servers. You can see the most important information about a server on the overview form. The task view contains different forms with which you can run the following tasks.

Specify Douments for Processing

Use the formular <Assign document owner> to specify the server documents that the users and groups will act as owner for. Use the form <Assign administrative documents> to specify which documents the users and groups may administer.

Specify Owner and Administrator Relations for the User Document

Configuration Parameter for Owner/Administrator Relations

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\Notes\SyncObjects\Notes ServerAdministrator	Server administrators (user, groups) are synchronized between target system and the Identity Manager database.

Assign the users and groups that may edit this server document using the form <Assign administrators>.

Add Lotus Notes Server to Lotus Notes Groups

Use the form <Assign groups> to add Lotus Notes servers to Lotus Notes groups.

Specify Lotus Notes Server Users

Us the form <Assign users> to specify which Lotus Notes user accounts user this server.

11

Managing an SAP R/3 Environment

- Introduction
- Setting Up SAP R/3 Synchronization
- Basic Configuration Data
- Managing User Accounts
- Groups, Profiles and Roles Administration
- Managing Structural Profiles
- Providing System Measurement Data

Introduction

The Identity Manager offers simplified user administration for the SAP R/3 environment. The Identity Manager concentrates on setting up and processing user accounts as well as groups, roles and profile assignments. The necessary data for system measurement is also represented in the Identity Manager. The data for system measurement is made available in the Identity Manager but the measurement itself takes place in the SAP R/3 system.

Company employees are provided with the necessary user accounts in the Identity Manager. Different mechanisms can be used to link employees to their user accounts. User accounts can also be managed separately from employees allowing administrator user accounts to be set up.

In order to provide the required permissions for user accounts, groups, roles and profiles are set up in the Identity Manager. The Identity Manager can not only assign user accounts to groups, profiles and roles but it can also add employees to them. In this case, the Identity Manager ensures that the appropriate group memberships are created for an employee's user account. So called products can be defined in Identity Manager. These group together groups, roles and profiles. These products are assigned to employees. This results in the assignment of employee's user accounts to group memberships. If user accounts in an SAP R/3 environment are maintained via the Central User Administration (CUA), access to client systems in the central system can be guaranteed or removed for user accounts in Identity Manager.

Setting Up SAP R/3 Synchronization

The Identity Manager supports synchronization with the SAP R/3 environment in the versions SAP Web Application Server 6.20 and 6.40 and SAP Netweaver Application Server 7.0. This ensures that all variations of the installation based on SAP ECC 5.0 and 6.0 are fully supported. Central User Administration is supported for all versions named here.

Identity Manager Service is responsible for synchronizing data between the Identity Manager database and SAP R/3. The application server ABAP must be installed as a prerequisite for using SAP synchronization. A system that is only based on a Java application server can not be accessed by the synchronizer.

Other prerequisites for synchronization are:

- Installation and configuration of a synchronization server
- Setting up a database for synchronization

If the server running the synchronization does not have a direct connection to the Identity Manager database, the synchronization is aborted with an error message.
Ensure that a direct connection to the Identity Manager database is possible!

The basic mechanisms for synchronization are explained in chapter Data Synchronization in Identity Manager on page 161.

SAP Synchronization Server Installation and Configuration

In order to set up a synchronization server, a server has to be provided that has the following software installed:

- Windows 2000 Server or Advanced Server with at least Service Pack 2 for Windows 2000, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 or Windows Server 2008 R2.

- Microsoft .NET Framework with at least version 3.5, service pack 1

- Microsoft Software Installation (MSI) service

- Identity Manager Service from the Setup CD
  This installation is described in the section Installing Identity Manager Tools on page 23. Please note the advice for installing on a terminal server (see Installing on a Microsoft Windows Terminal Server on page 25).

- Java Runtime Engine with at least version 1.4.2_04

- The following DLL's have to be available in the system directory (System32):
  - LibRFC32.dll
  - MSVCP71.dll
  - msvcr71.dll
  - mfc71u.dll
  - mfc71.dll

Then, Identity Manager Service needs to be configured and started on the synchronization server. Read the section Setting Up a Server for Database Access on page 44 for more information.

Other steps are:

- Set up the system information and an client for synchronization
  The minimum required information is:
  - R/3 host name
  - System number
  - Client number (client) and language
  - Central system ID when synchronizing a CUA

- Provide an administrator user account for the synchronization (user ID with associated password)
  The permissions required for this administrator user account are listed in section Permissions Required for SAP R/3 Synchronisation on page 346.

In the SAP R/3 versions up to and including versions 6.20 and 6.40, the password and user input are not case sensitive. These passwords are no longer valid as from SAP R/3 Netweaver Application Server 7.0, passwords are case sensitive. All SAP's own tools that are supplied up to SAP Web Application Server 6.40, apart from the SAP GUI (RFC-SDK, SAP.NET Connector), change the password to capital letters before passing them to SAP. If this is done, all the usual tools can be accessed on SAP Netweaver Application Server 7.0 by RFC.

Installing the Identity Manager Business Application Programing Interface

In order to access SAP R/3 environment data and business processes with Identity Manager, the supplied Business Application Programming Interface (BAPI) has to be installed on the system. You can find the necessary transport file on the Identity Manager setup CD in directory "...\Redistributables\SAP\SAPTransport". Certain files contain additional Addon files and installation instructions.

Apply the BAPI transport as follows:

- SAPTRANSPORT_47.ZIP – compatible to versions SAP Web Application Server 6.20

- SAPTRANSPORT_70.ZIP – compatible to versions SAP Web Application Server 6.4 and SAP Netweaver Application Server 7.0 (SAP ECC 5.0 and 6.0)

If your system supports unicode, select the transport package for the unicode. Archive files also contains transport packages for systems in separate directories that do not support unicode.

Permissions Required for SAP R/3 Synchronisation

It is recommended that you set up an administrator user account identically on all system/client combinations for synchronization. The administrator should have a user type of ”Dialog“ or ”Communication“ to read out other information.

The rights described in the following are expected for the user account so that both read and write access is available for the system. If only read access should be permitted, we recommend setting up a profile which has executable permission for transactions SU01 and PFCG but prevents writing at activity or field level. Set the user account access permissions on the client system to ”DUMMY“ if the systems in the Central User Administration should be synchronized.

Apart from executable rights, the user account has to get all objects from the authorization classes ”ZVIH“, ”ZVIA“, and ”ZVIL“ which are installed by the transport package for synchronization. The transport file that we provide ”SAPRole.zip“ includes a transport with an role that base authorization object already has. This role can be assigned to the user account for synchronization. You can find the transport file on the Identity Manager setup CD in directory ”...\Redistributibles\SAP\SAPTransport“.

If it is necessary to generate a proxy DLL to access the USER building block in the system, the authorization ”S_DEVELOP“ (activity 03) is generated on a one of basis in addition.

Required Authorization Objects and their Meaning:

- S_TCODE with a minimum of transaction codes SU01, SU53, PFCG
- S_ADDRESS1 with activities 01, 02, 03, 06 and valid address groups (min. ”BC01“)
- S_USER_AGR (role maintenance) with activities 02, 03, 22, 78 possibly with restrictions in name ranges (e.g. ”Z*“)
- S_USER_GRP (group maintenance) with activities 02, 03, 05, 22
- S_USER_AUT (authorizations) with activities 03, 08
- S_USER_PRO (profile) with activities 01, 02, 03, 22
- S_USER_SAS (system specific assignments) with activities 01, 06, 22
- S_RFC (authorization check by RFC access) with activity 16 at least for function groups ZVI, /VIAENET/ZVI0, /VIAENET/ZVI_L, /VIAENET/Z_HR, SU_USER, SYST and SDTX
- S_TABU_DIS (use of standard tools like SM30 for maintaining tables) with activity 03

Setting Up the Identity Manager database for SAP R/3 Synchronisation

Configuration Parameters for SAP R/3 Synchronization

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3	SAP is supported. Preprocessor relevant configuration parameter. Changes to the parameter require recompiling the database.

Prerequisites for synchronizing an SAP R/3 environment with the Identity Manager database are:

- The configuration parameter ”TargetSystem\SAPR3“ is set. This releases the SAP components of the database for use with Identity Manager tools.
  The configuration parameter ”TargetSystem\SAPR3“ is a preprocessor relevant configuration parameter. This means that the database has to be compiled after changing this parameter. For more information read the section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual.

- The synchronization server is set up.
  Installation prerequisites are described in section SAP Synchronization Server Installation and Configuration on page 344. How to set up the server in the Identity Manager database is explained in section Declaring the Synchronization Server on page 348.

- Set up the system to be synchronized in the Identity Manager database.
  Refer to section System Setup in the Identity Manager Database on page 349.

- Set up the clients to be synchronization in the Identity Manager database.
  Read section Client Synchronization Setup on page 352.

- Synchronization configure and start.
  Use the synchronization configuration to specify which of the SAP R/3 objects are synchronized between the target system and the Identity Manager database. Read section Client Synchronization Setup on page 352 for more information.

Target System Wizard for Identity Manager Database Synchronization with SAP R/3

Tool: Manager

In the category <My Identity Manager>\<Target System Wizard>\<Configure SAP R/3> in Manager there is a wizard to help set up the Identity Manager database for synchronization with an SAP R/3 environment. The assistant includes the most important configuration steps for putting synchronization into operation. The wizard takes you through the configuration steps from setting up the system in the Identity Manager database through to synchronization. Basically, the assistant does not make any settings to Notes that are managed by Identity Manager. All settings are changes to Identity Manager behavior and are saved in the Identity Manager database.

The following steps are carried out by the wizard:

- Set up an system within the database or
  configure an existing system in the database

- Set up an client in the database or
  select an existing client in the database.
- Set up the sychronization server in the database
- Set up a user account resource
- Starts the initial synchronization

After the wizard is completed, other configuration steps may be necessary in order to manage the SAP R/3 environment in Identity Manager.

Declaring the Synchronization Server

Tools: Manager; Identity Manager with application role <Target system>/<SAP R/3>

All Identity Manager Service actions are executed on the synchronization server. The entries that are relevant for synchronization and administration with the Identity Manager database are processed by the synchronization server.

Set up the server hardware in the category <SAP R/3>\<Basic configuration data>\<Server>. A minimum of the following data is required for the server hardware:

- Server name
  Server identifier
  The queue name for the corresponding Job Server is formatted from the server name. The process steps are requested by the Job Queue using exactly this name.
- Server hardware
  The server hardware is preset by when you select the server.
- Server language

The meaning of the other input fields and option is described in section Synchronization Server Administration on page 196. However, this input is not relevant for the server to function as a synchronization server.

Once the synchronization server has been added to the database, a corresponding entry is made for a Job server that will be responsible for supplying the queue for handling the target system specific processes with Identity Manager Service. This queue needs to be entered into the Identity Manager Service configuration file. Refer to section Configuring a Job Server on page 210 in the Configuration Manual.

System Setup in the Identity Manager Database

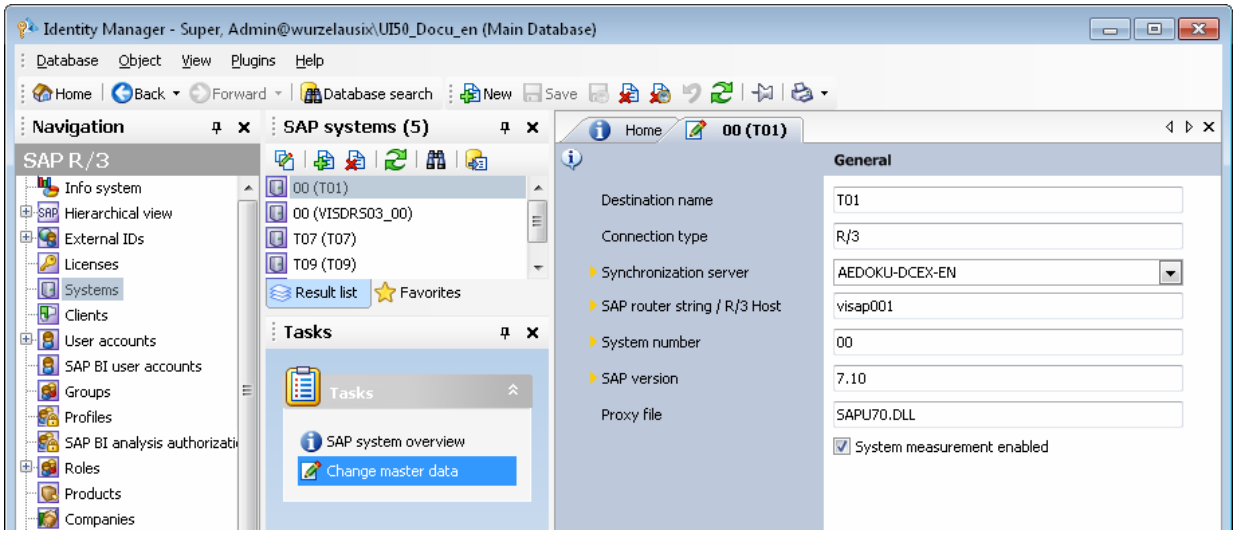
Tools: Identity Manager with the application role <Target system>\<SAP R/3>, Manager

Configuration Parameters for Setting Up an System

CONFIGURATION PARAMETER	MEANING
TargetSystem\SAPR3\Versions	Specifies the installed SAP versions. For each installed version of SAP, a configuration parameter is expected below this configuration parameter that supplies the DLL containing the RFC proxy for the system to be activated. The required configuration parameter is already preset in some systems.

The system setup is prerequisite for Identity Manager database synchronization with the SAP R/3 environnment. Declare the systems in the category <SAP R/3>\<Systems>.

Setting up a System



The following data is required for an system:

- System ID
  Enter the name of the system.
- Connection type
  Enter ”R/3“ as target system connection type.
- Synchronization server
  Select the server that should word as synchronization server for this system.
- SAP router string / R/3-Host
  As R/3 host name, enter the SAP R/3 application server IP address, the SAP R/3 application network name or the SAP router string with name or IP address of an SAP R/3 application server appended.
- system number

- SAP version
  Enter the version number of your system here. The version number is required to determine the appropriate DLL containing the RFC proxy for the system to be controlled. The configuration parameter ”TargetSystem\SAPR3\Versions“ is required for this.

- Proxy file
  If the DLL that contains the RFC proxy for the system to be controlled, is not equivalent to the default, the DLL to be used is entered here.

- Enable system measurement
  Set this option when you want to run a system measurement for this system. The Identity Manager provides the measurement data but the actual system measurement takes place in the SAP R/3 environment.

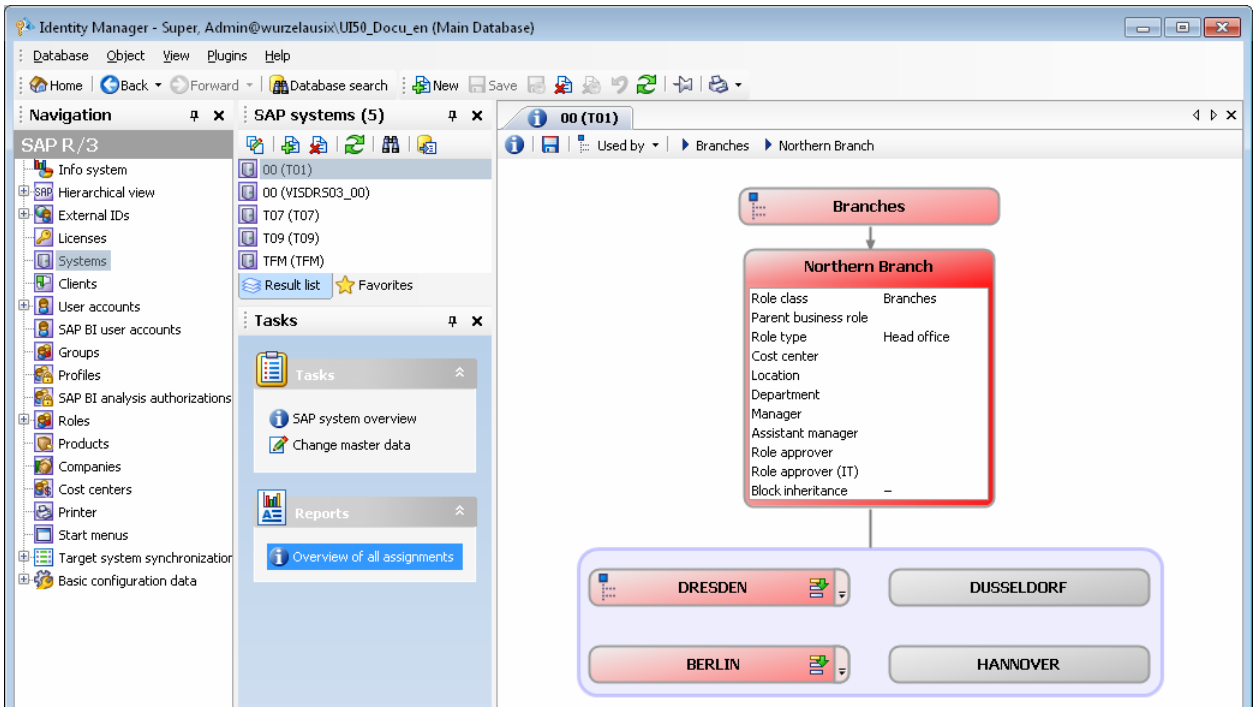
System Reporting

The Identity Manager provides several reports containing information about the selected root object and its relations to other objects in the the Identity Manager data. The following reports are available for systems.

Overview of All Assignments

This report shows all employees that are assigned to at least one user account in the selected system. Directly assigned objects as well as those object inherited by the employee are take into account in this case. The report shows which roles of a role class the employee belongs to. What you get is an organigram of the different role classes for the selected system.

Report ”Overview of all Assignments“ for a System



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees in the system that have a user account and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

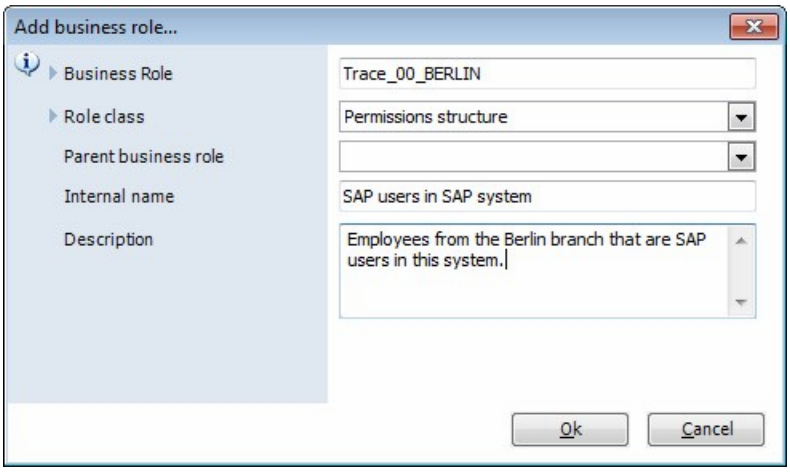
Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

Bookmark Employee for Tracking

To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system and the role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by The Identity Manager to decide whether you want to display the business role straight away or not. If you confirm

the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Client Synchronization Setup

Tools: Identity Manager with the application role <Target System>\<SAP R/3>, Manager

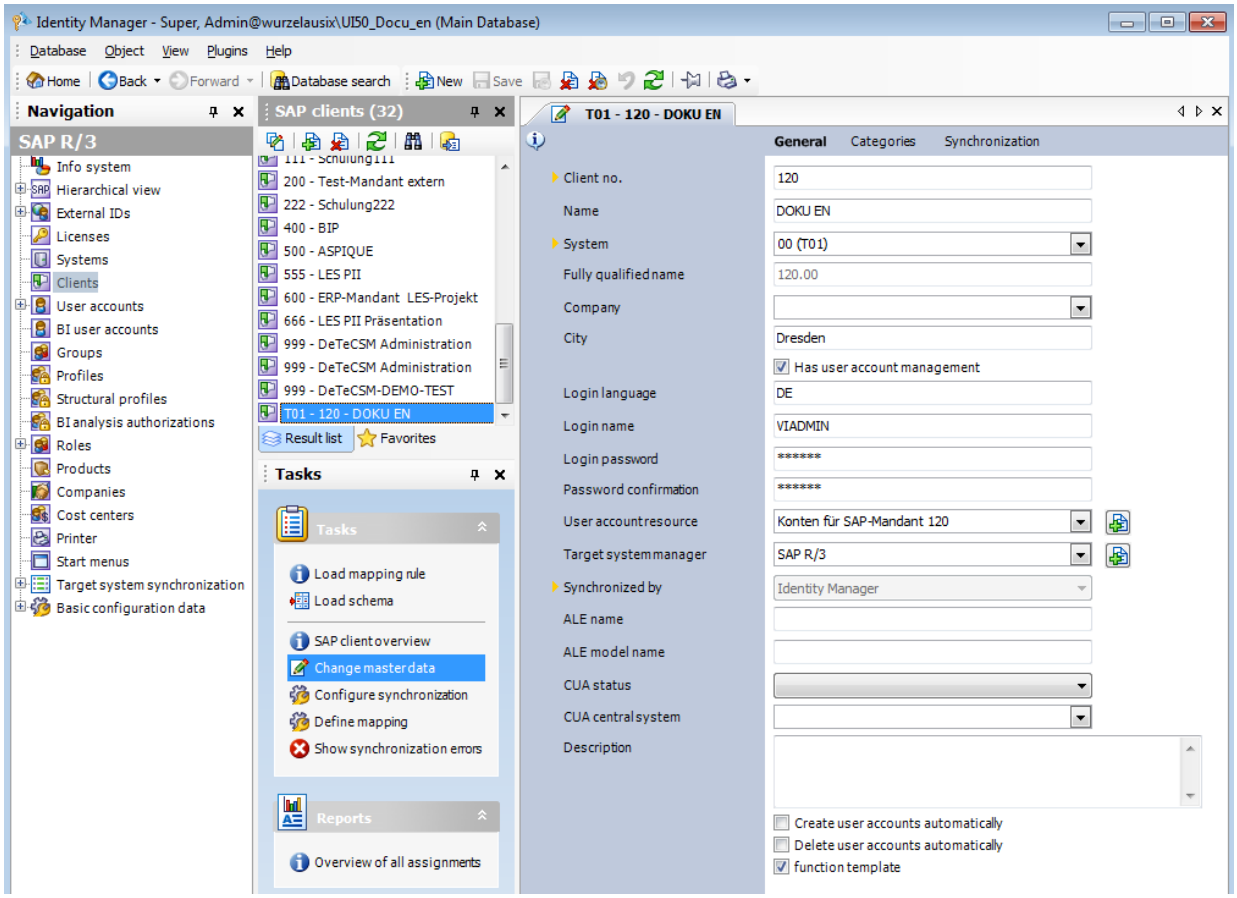
Access to the system with defined clients is necessary for user administration and synchronization. clients are only read from of the SAP R/3 environment during synchronization. An exception is the client that is used for synchronization. You have to set up this client in The Identity Manager before synchronization can be started.

Add the clients for synchronization in the category <SAP R/3>\<Clients>. Enter the required data for an client on the form <Change master data>.

General Master Data for a Client

Enter general master data for an client on the <General> tab.

Setting Up a Client



The following input is required for the clients:

- client number and name

- System
  Assignment to the system

- Fully qualified name
  The fully qualified client name is created automatically from the client number and the system

- Company location
  The company address given here is used when a new user account is set up.

- Has user account management
  Specify whether the client will be used for user administration
  You have to set this option for the clients that are going to be synchronized.

- Login language
  The selected language for the synchronizer's login determines the language of the description text for all SAP objects for this client. So that when you select "EN" all the text from groups, roles, profiles and start menus is in English.

- Login name, password and confirmation
  Enter the administrator user account for synchronization and its password for logging into the Identity Manager Service.

- User account resource
  This input is necessary when you manage the user account with a user account resource in an area of a target system. Read the section Managing user accounts with User Account Resources on page 374 for more information.

- Target system manager
  Select an application role in the Identity Manager whose members are managers for this client. User the button next to the input field to create a new application role.
  Target system managers can only edit client objects that are assigned to them.

- Synchronized by
  Specify how the data will be synchronized between the system and the Identity Manager. Choose between "Identity Manager", "FIM" and "No synchronization".

  Identity Manager: data synchronization between the Identity Manager database and the system is carried out by the synchronization components from the Identity Manager.
  FIM: data synchronization between the Identity Manager database and the system is carried out by the Microsoft Forefront Identity Manager.
  No synchronization: no changes are automatically transfered from the Identity Manager database to the system.

  You can only specify the type of synchronization when a new client is added. Once it has been saved, no changes can be made. If you select "No synchronization" you can define custom processes to exchange data between the Identity Manager and the system.

- ALE name
  Name used to map the client as logical system in the SAP distribution model.

- ALE model name
  Name of the SAP distribution model that maps the relation between the logical systems of the Central User Administration (CUA).

- CUA Status
  Labels client usage when CUA is enabled. Possible values are "Central", "Client" and "None". If CUA is not enabled, do not enter a value. For more information see section Special Features of Synchronizing with a CUA Central System on page 360.

- CUA central system
  Assign a valid central system to clients that have CUA status ”Client“.

- Description
  Additional information about clients.

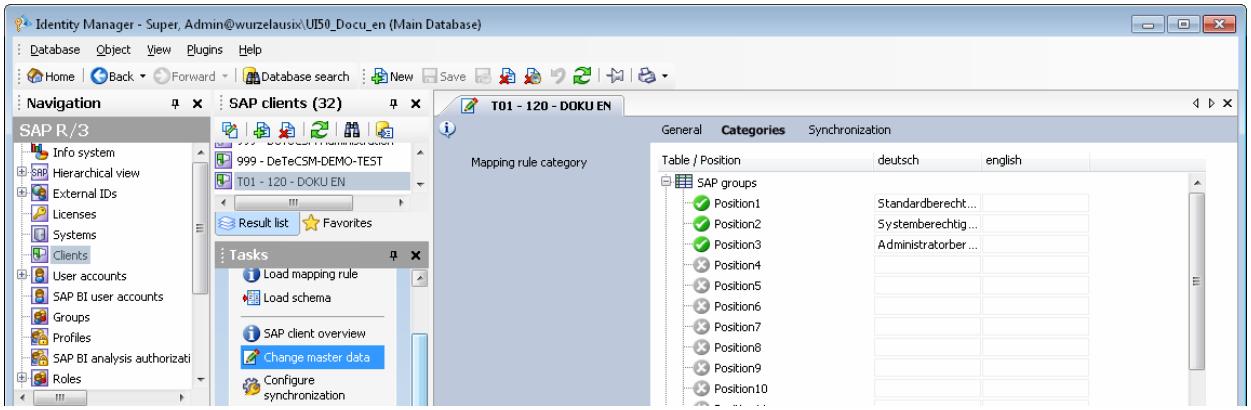
- Create user automatically, delete user automatically
  Specify whether user accounts should be automatically created or deleted in the clients. These options are only shown when the configuration parameter ”TargetSystem\SAPR3\PersonInheriteSAPGroup“ is enabled. You can only edit the options if the client has a user account resource. The options are not available for CUA central systems. You can find more information in the section Automatically Adding and Deleting user accounts by Changing Group Memberships on page 380.

- Function template
  If this option is enabled the client‘s data is used as a value template for the Permissions Editor when SAP functions are set up.

Specifying Categories

Use the tab <Categories> to define categories for groups and user accounts. Categories are relevant when a user account inherits groups. Groups can be selectively inherited by the user account. To do this, groups and user accounts are divided into groups. The inheritance principle is described in more detail in section Inheriting Group Memberships Based on Categories on page 82.

Defining Categories



You define categories as follows:

- Open the membership tree for the table you want.

- Enable a position.

- Enter a name for the category in the column with the respective login language.

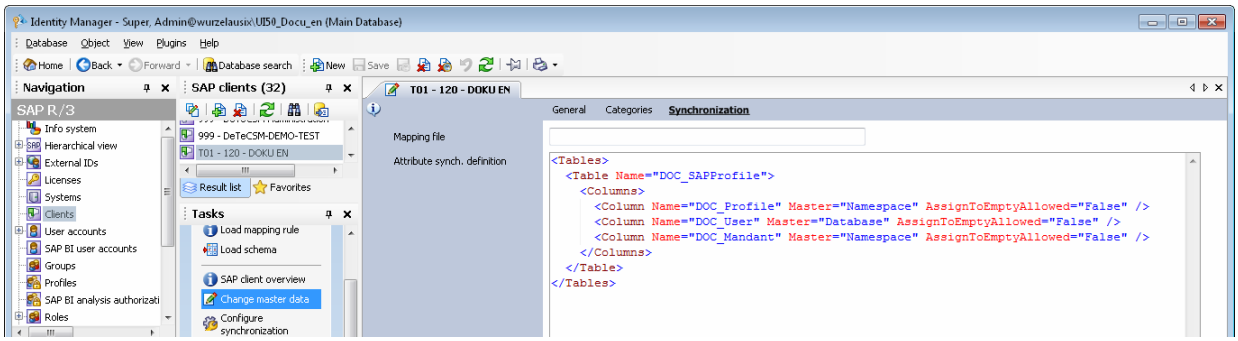
Customizing Data Synchronization

On the <Synchronization> tab you can make special adjustments for synchronizing the data between the Identity Manager database and the target system. Since the requirements within an SAP R/3 environment may be different from client to client, you can make changes to each client individually.

The mapping file contains the templates for mapping target system specific objects, such as user accounts, groups or hardware objects, between the Identity Manager database and clients. The evaluation is carried out using target system specific process components. An external mapping file only has

to be given if the default mapping for the data should not be used. This external mapping file must exist on the synchronization server. If no path is given, the mapping file has to be in the Identity Manager Service install directory on the synchronization server. Refer to the chapter Customizing Mapping rules on page 180 for further infomation.

Customizing Data Synchronization



You can specify the master for data synchronization for individual target specific object properties with the attribute synchronization definition. The input is entered in an XML statement. Define the data master on the form <Mapping definition>. You can also customize the master definition in the XML statement. These changes are shown in the mapping editor after saving. For more information see section Specifying the Data Master for Object Properties

Reports about Clients

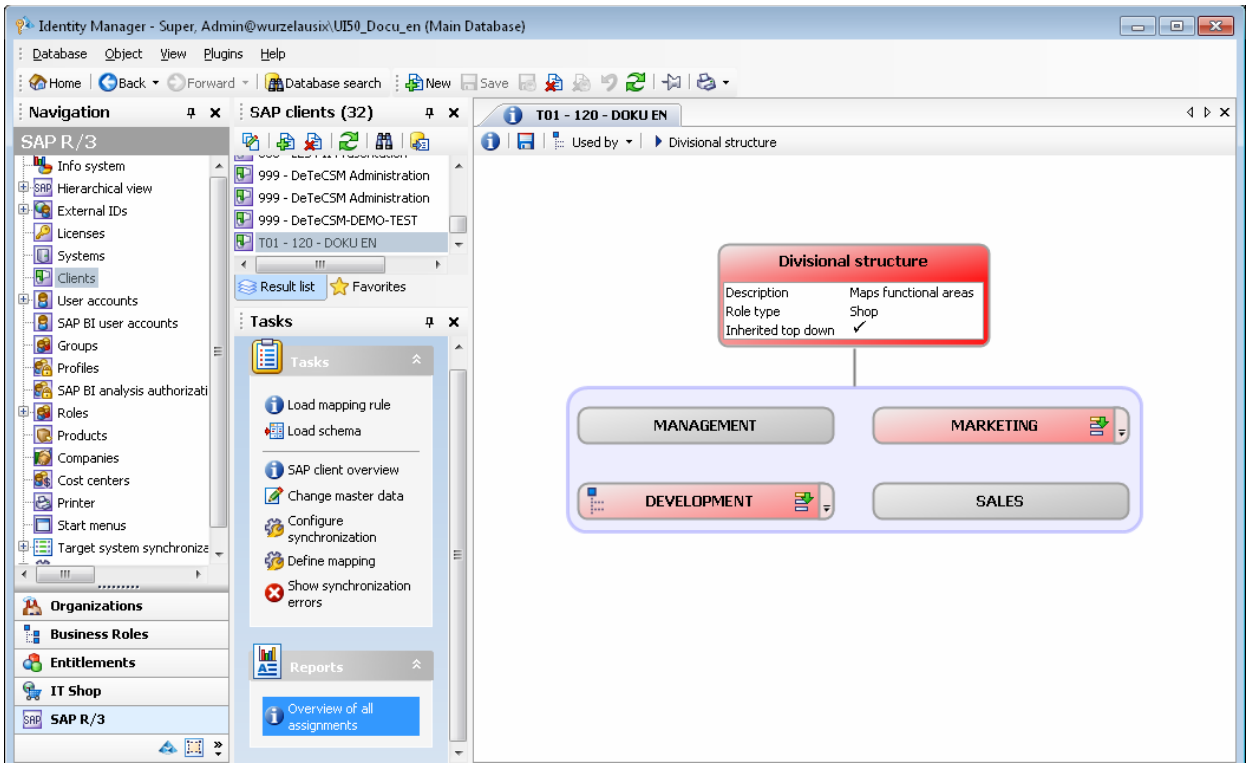
The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for clients

Overview of all Assignments

This report shows all employees that are assigned to at least one user account in the selected client. Directly assigned objects as well as those object inherited by the employee are take into account in this

case. The report shows which roles of a role class the employee belongs to. What you get is an organigram of the different role classes for the selected client

Report „Overview of all Assignments" for a Client



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that have a user account in the selected client and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

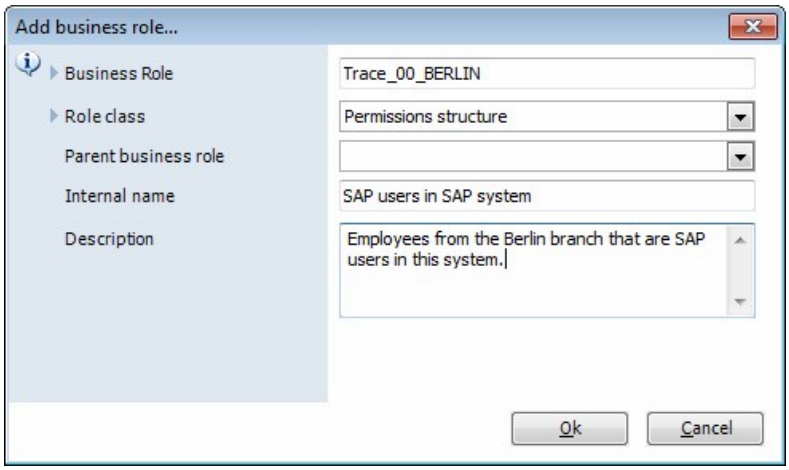
Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

Bookmark Employee for Tracking

To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Configuring Client Synchronization

Tool: Manager

Take the basic information about data synchronization from the section Data Synchronization in Identity Manager on page 161. The following steps are required to synchronize between an Identity Manager database with an SAP R/3 environment:

- Customize configuration parameters that are relevant for synchronization.
  For more information read section Configuration Parameters for Synchronization with an SAP R/3 Environment on page 358.

- Configure synchronization.
  The basic procedure is described in section Data Synchronization in Identity Manager on page 161. Speical feature of synchronization with an client are given in section Special Features of Client Synchronization Configuration on page 358.

- Define a mapping
  The basic procedure is described in section How to Define a Mapping on page 175.

Refer to section Synchronization Analysis on page 176 for detailed information about synchronization and handling of synchronization objects.

Configuration Parameters for Synchronization with an SAP R/3 Environment

The following table only lists configuration parameters that are relevant for scheduled synchronization. There may also be other configuration parameters be applied for target system relevant actions, for example, inserting, changing or deleting a user account in the database and the subsequent transfer into the target system via Identity Manager Service.

The complete list of configuration parameter is found in Designer. Edit configuration parameters in Designer. For more information, read chapter System Configuration Parameters on page 214 in the Configuration Manual.

Certain configuration parameters are preprocessor relevant. You have to compile the database if you make any changes to these parameters. Read section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and section Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual for more information.

Configuration Parameters for Synchronizing a Client

CONFIGURATION PARAMETERS	MEANING
TargetSystem\SAPR3\MaxFullsyncDuration	Specifies a timeout for synchronization.
TargetSystem\SAPR3\PersonAutoFullsync	Depending on this parameter the decision is made as to whether automatic assignment of employees should come into effect when a user account is added during synchronization.

Special Features of Client Synchronization Configuration

Read section Data Synchronization in Identity Manager on page 161 for details about the basic synchronization configuration. At this point, we are only going to look at the special features relevant to the synchronization configuration for clients. The following configuration tasks are available for synchronizating an client.

Configuring Synchronization

Use this form to set up the synchronization configuration. Enter the basic synchronization configuration and the schedule on the <General> tab. If necessary, you can manually start synchronization from here. On the <Synchronization> tab, specify how objects should be handled during synchronization.

The following options are available on the <Additional settings> pane on the <General> tab:

- Only synchronize enabled profiles
  If this option is set, only active profiles are synchronized. If the option is not set, all profiles are synchronized.

- Only synchronize roles with current validity period
  If this option is set, only role assignments whose validity periods are include the current date are included. This makes sense in connection with the option <Remove invalid role or profile assignments> to clean up historical role assignments to user accounts. If the option is not set, all role assignments are included.

- Remove invalid role or profile assignments
  If this option is set, the corresponding list in the system is completely deleted and rebuild each time a user account group, role or profile assignment is changed. This makes sense in connection with the option <Only synchronize role assignments with current validity period> to clean up historical entries in the role assignment list. If the option is not set, only affected entries are added or removed when changes are made to the user account's group, role or profile assignments.

- Synchronizes system measurement data(...)
  If this option is set, system inventory data is synchronized.

Take note of the following before you enable the object type AUTHX on the <Synchronization> form in the <Synchronized object types and assignements>:

Synchronization of the authorization fields (object type AUTHX) results in the synchronization of values ranges and look-up tables!
This is a large amount of data. The process of loading it can take a while.

When you specify the data master for object types and assignments, take into account the restrictions kept in the mapping for target system synchronization. Restrictions are defined on the column mapping and the options <Target system property can be edited> and <Database column can be edited>. See section Special Cases of Synchronization, page 194 ff for more information.

Only changes to user accounts from Identity Manager can be written to the SAP R/3 system in the default installation. Refer to the column mapping for the object type USER to find out which object properties are exempted from this.

Defining a Mapping

Use this task to specify how the structure of properties belonging to the object types to be synchronized is mapped in the database and in the target system. The configuration of assignments is described in detail in section How to Define a Mapping on page 175.

Displaying Synchronization Errors

This task provides an alternative method for analysing the synchronization in addition to the Identity Manager Service log file. The SAP R/3 objects and dependencies which failed during synchronization are shown on the form. A detailed description of the error is displayed. The section Logging Synchronization Errors on page 176 provides more detailed information.

Special Features of Synchronizing with a CUA Central System

- Only roles and profiles from the client system that correspond to the login language for the administrator user account for synchronization are mapped in the Identity Manager!
- Single roles or profiles are not synchronized.
- Maintain all client system roles and profiles from the system in the language given as <Login language> in the central system client in the Identity Manager.

If a Central User Administration is connected to the Identity Manager, it is only necessary to synchronize with the central system. To do this, the client must be labeled as central system (input field <CUA status>, value <Central>). During synchronization the Application Link Enabling (ALE) distribution model is loaded and tries to assign all clients that are configured as client system to the central system in the Identity Manager. At the same time, all clients that are in the same system as the central system are added automatically in Identity Manager and assigned to the central system (input field <CUA central system>). All clients that are in another system have to exist in Identity Manager at this time. These clients could have been manually added to the Identity Manager as well as though synchronization.

If a text comparison between roles and profile is run between child systems and the central system in an system, the child system roles and profiles are only assigned in to user accounts in the central system. The Identity Manager prohibits adding and modifying of user accounts in CUA child systems.

When a text comparison of roles and profile is made between the child and central system in the system, the roles and profiles are saved on a language dependent basis in the table ”USRSYSACTT“. Only those roles and profiles that correspond to the login language of the administrator user account for synchronization are loaded from the table ”USRSYSACTT“ when synchronizing with the Identity Manager. If there are any entries that are not maintained in this language, they are not transfered to the Identity Manager. So that all roles and profiles from the child system that are mapped in the Identity Manager they need to be maintained in the language saved for the central system client in <Login language> (see section General Master Data for a Client on page 352).

Restricting Synchronization Objects Using User Permissions

The Identity Manager offers the possibility to restrict user account and groups for synchronization by using user permissions. In this case, only the user accounts and groups are synchronized that the administrator user account for synchronization is authorized for. All other groups and user accounts are filtered out of the user lists and the groups list of the function module ”/VIAENET/U“. If only a small part of the user account in the SAP R/3 environment should be synchronized with the Identity Manager then the synchronization can be accelerated with this method.

Prerequisite:

- The administative user account for synchronization is assigned exactly those groups in the authorization object S_USER_GRP, characteristic CLASS, that should be synchronized.
- There are user accounts that one of these groups is assigned to in the SAP R/3 environment as user group for testing authorization (in the login data).

- The administrator user account for synchronization is entered in the Identity Manager as <Login name> for the client to synchronize.

During synchronization, the groups are loaded into the Identity Manager database that the adminstration user account for synchronization has access to in the authorization object SUSER_GRP. All user accounts that are assigned one of these groups as user group for authorization testing are also synchronized. All other groups and user account are handled by the synchronization like non-existant objects in target system (see section Synchronization Behavior for Selected Objects on page 170).

Basic Configuration Data

Target System Manager

In the Identity Manager, you can assign employees to every client that can edit objects for this client in the Identity Manager. To do this, assign a <Target system manager> application role in the client master data. Then assign employees that are authorized to edit the client in the Identity Manager to this application role.

Edit target system managers for SAP R/3 in the Manager in the category <SAP R/3>\<Basic configuration data> or in Identity Manager in the category <Identity Manager administration>\<Target systems>\<SAP R/3>. You can find more detailed information about application roles in the section The Identity Manager Roles Model on page 61. Refer to section General Master Data for a Client on page 352 to find out about assigning target system managers to clients.

Managing User Accounts

You can manage the users of an SAP R/3 environment with the Identity Manager. The Identity Manager concentrates on setting up and editing user accounts. Groups, roles and profiles are represented in the Identity Manager, in order to provide the necessary permissions for user accounts. Other data that is required for system measurement is also displayed. Although the measurement data is kept in the Identity Manager, the actual measurement takes place in the SAP R/3 environment.

Prerequisite for managing user accounts with the Identity Manager is to set up a synchronization the required clients.

The Identity Manager works with several methods to create user accounts and assign them to employees.

- Employees and user accounts can be manually entered and assigned to each other
- Employees automatically obtain their user accounts through user account resources. If an employee does not have a user account in an client, it is created by assigning a user account resource to an employee using the inheritance mechanism integrated into the Identity Manager and subsequently processing a new user account. This method is described in more detail in section Managing user accounts with User Account Resources on page 374.
- When a user account is added, an existing employee is automatically assigned or created if necessary. The employee master data is created based on the existing user accounts. This mechanism can be used when a new user account is created either by manually adding it or by synchronization. This is, however, not the default method for the Identity Manager. This method is explained in the section Automatic Assignment of Employees to User Accounts on page 40.

The basic mechanisms are dealt with in the chapter Employees and User Accounts on page 25.

Basic Data for User Account Administration

The Identity Manager already supplies certain basic data for user administration with migration. This includes:

- User account types
- Types for external identification

Other basic data is read from the SAP R/3 environment during synchronization and cannot be edited in the Identity Manager. This merely allows assignment to a user account.

This basic data consists of:

User Account Basic Data

BASIC DATA	OBJECT TYPES	CORRESPONDING CONFIGURATION PARAMETER
Licenses	LICENSETYPE	TargetSystem\SAPR3\SyncObjects\Licensetype
Printer	PRINTER	TargetSystem\SAPR3\SyncObjects\Printer
Cost centers	PROFITCENTER	TargetSystem\SAPR3\SyncObjects\ProfitCenter
Start menus	STARTMENUE	TargetSystem\SAPR3\SyncObjects\Startmenue
Company addresses	COMPANY	TargetSystem\SAPR3\SyncObjects\Company
Login language	LOGINLANGUAGE	TargetSystem\SAPR3\SyncObjects\LoginLanguage
Roles	ROLE	TargetSystem\SAPR3\SyncObjects\Role
Groups	GROUP	TargetSystem\SAPR3\SyncObjects\Group
Profiles	PROFILE	TargetSystem\SAPR3\SyncObjects\Profile

The following section provides a short description for some of the basic data. You can find more detailed explanations in the SAP R/3 system documentation.

User Account Types

User account types are supplied by default by the Identity Manager during migration. SAP R/3 acknowledges the user types listed below:

User Account Types

USER ACCOUNT TYPES	MEANING
Dialog (A)	This user type labels normal system user in an system.
System (B)	This user type is used for backgroand processing and communication within an system.
Communication (C)	This user type is used for dialog-free communication between systems.
Service (S)	This user type is used for general user accounts and for anonymous system access. User accounts of this type should have heavily restricted permissions.
Reference (L)	This user type is also used for general user accounts and only serves to issue additional permissions.

Types for External Identification

Configuration Parameter for External User Identification

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\UserDefaults\ExtID	Specifies the default user type for external identification of user accounts.

External authentication methods for for logging on to an system can be used in SAP R/3. The Identity Manager supplies the following type as user identifiers to find the login data necessary for different authentication mechanisms for external systems on an system:

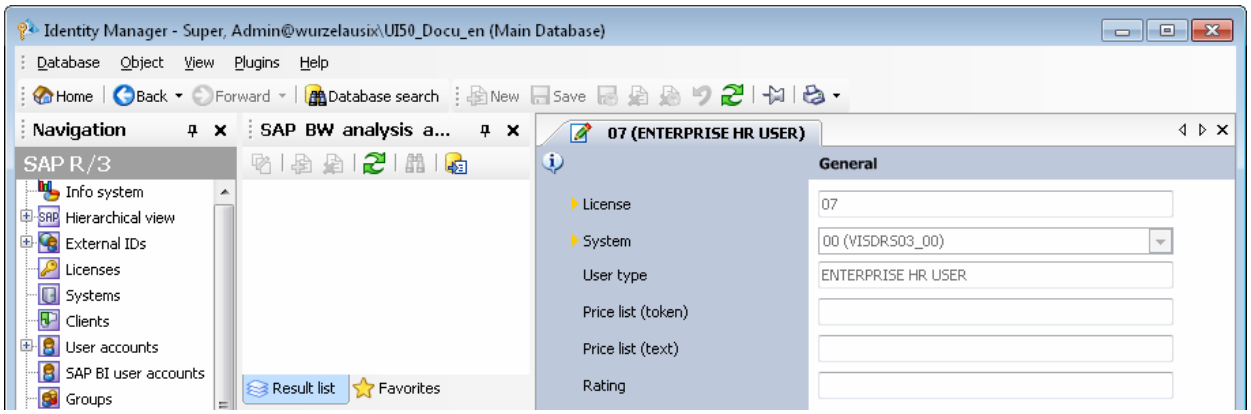
- DN - distinguished name for X.509
- NT - Windows NTLM or password verification with the Windows domain controler
- LD - LDAP bind <user defined> (For other external authentication mechanisms)

Use the configuration parameter TargetSystem\SAPR3\UserDefaults\ExtID to specify which type of external ID is selected by default when one is added.

Licenses

Licenses are required for the user system measurement. Licenses are displayed in the category <SAP R/3>\<Licenses>.

Displaying Licenses



The following information is shown for Licenses:

- License name
  Unique license identifier
  Is used to determine the system measurement rating if no license rating is entered.
- Associated system
- User type
- License price informationen

- Rating
  The license rating is not listed in the SAP R/3 environment but has to be entered directly by the user. The license rating is evaluated when the system measurement ratings are determined. If no rating is entered the license ID for determining the rating for system measurement is used.
  Enter any alphanumeric character string. Determining system measurement rating is not case sensitive.

SAP Printers

Printers are displayed in the category <SAP R/3>\<Printer>. The following information is shown:

- Location and description of the printer
- Associated client
- Device type name
- Output device for the spooler
- Assigned user accounts

SAP Cost Centers

The cost centers are shown in the category <DAP R/3>\<Cost centers> and contain the following data:

- Cost center name and description
- Associated cost code
- Associated client
- Cost center validity period

SAP Start Menus

Start menus are displayed in the category <SAP R/3>\<Start menus> and include the following information:

- Start menu name
- Associated client
- Detailed description
- Assigned user accounts

SAP Company Addresses

Company addresses are displayed in the category <SAP R/3>\<Companies> and include the following information:

- Company name and short name
- Associated client
- Address number

- City
- Search pattern
- Assigned user accounts

SAP Login Language

SAP login languages are stored in the category <SAP R/3>\<Basic configuration data>\<login languages> and include the following information.

- Name of the login language and language key
- Assignments to system
- Assignments to user accounts

Entering User Account Master Data

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Configuration Parameters for Setting Up User Accounts

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\PersonAutoDefault	Specifies whether automatic assignment of employee should come into effect when a user account is added /changed (not active for synchronization).
TargetSystem\SAPR3\UserDefaults	When this configuration parameter is set, default values should be used for user accounts.
TargetSystem\SAPR3\RedoDelay	This configuration parameter specifies the delay time after which an incompleted update is repeated. The input is in minutes.

A user account can be linked to an employee in the Identity Manager. You can also manage user accounts separately from employees, for example, to allow administrative user accounts to be set up.

The user accounts are displayed in the category <SAP R/3>\<User accounts>. You can enter the necessary data for user accounts on the <Change master data> form and rework it if necessary. Ensure that you fill in all the compulsory fields.

We recommend using user account resources to set up a user account for a company employee. If you do use a user account resource to set up the user, some of the master data that is described in the following is created using templates. The range, in this case, is based on the default manage level for the user accounts resource. The templates supplied should be customized as required.

General Master Data for a User Account

If user accounts are maintained through a Central User Administration you can only add user accounts to clients that are labeled for a central system.

Enter general data for a user account on the <Address> tab. You can assign an employee to a user account from the <Employee> menu. If the user account was created using a user account resource, an employee will already be entered. If you use automatic employee assignment, a associated employee is created and entered into the user account when the user account is saved. If you do not use any of these methods but manually create the user account, you can also assign an employee manually to the user account.

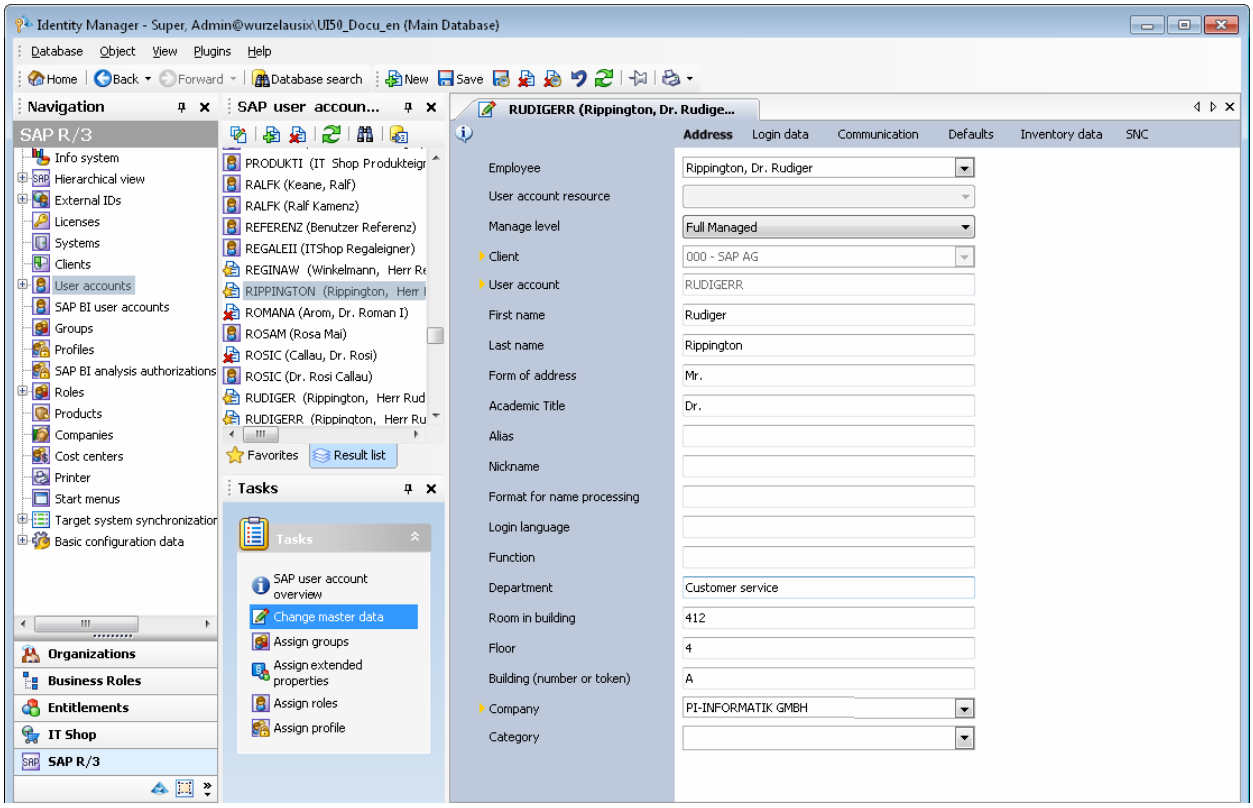
When user account resources are assigned to an employee or a resource to a company structure, an associated user account is created with the integrated inheritance mechanism and the process handling that follows. If the process handling fails because, for example, not all the neccesary IT operating data could be found, you can also create the user account manually and, at the same time, select the user account resource to use. The menu <User account resources> showthe user account resources offered by the target system.

The user account manage level is decided by the range of employee's properties that are passed on to the user account. The Identity Manager's default installation is configured for the manage levels "Unmanaged" and "Full managed". User accounts with the manage level "Unmanaged" are merely linked to an employee but do not inherit other properties. User accounts with the manage level "Full managed" inherit defined employee properties. You can define other manage levels depending on the company's requirements.

When user account resource is assigned to an employee, the default manage level is used to create the user account resource. Normally, the manage level "Full managed" is used as default. If you create the user account with automatic employee assignment, the manage level is "Unmanaged". You can change

the levels after the user account has been saved using the menu <Manage level>, provided that the client has a user account resource.

User Account- Address Data



Enter the following data for a user account:

- Employee
  Assign an employee to the user account. If the user account is created using a user account resource the employee is already entered. If you create the user account manually, you can select the employee from a list.

- User account resource
  Select a user account resource from the list. If you have entered an employee in the <Employee> input field, the Identity Manager finds the IT operating data for this employee and enters it into the corresponding user account fields. Use the user account resource to automatically fill the user account fields and to define a manage level for the user account. To ensure future maintenance of the user account through user account resources, allocate the target system type and the employee to the user account resource.

- Manage level
  Select a manage level from the drop-down menu. You can only enter the manage level when you have already entered a user account resource. The values in the list are dependent on the manage level defined for the selected user account resource. You can find further informationin the section Specifying Manage Levels for Handling User Accounts on page 377.

- Client
  The client to be added in the user account. You can only edit this input field when the user account is added.

- User account
  Enter a user account name. If you have assigned a user account resource the user account name is mapped from the employee's main user account depending on the manage level.

- First name, last name
  Enter the first and last names. If you have assigned a user account resource, the input fields are automatically filled out depending on the manage level.

- Salutation, academic title, alias, nickname
  Additional information to the user account.
  The alias is an alternative ID for the user account that is used as log in for certain internet transactions.

- Format for name editing, login language
  Format and country for name editing
  The format and country for name editing define the edit rule for formatting the full name of the employee in the SAP target system. The name editing format specifies the order in which parts of names are put together so that an employee's name is represented in an extensively long form. The country together with the name editing format key provides the means to uniquely identify a editing rule.

- Function, department
  Additional information about the user account. Used when addresses are printed.

- Room#, level, building
  Additional information about the user account.

- Company
  The company that the user account is assigned to.
  When a user account is added, the default company address of the client is used. If the client does not have a default company address then the company address with the smallest address number is found and assigned to the user account.

- Risk index
  Average of all risk index values for assign groups, roles, profiles and structural profiles.
  This input fields is only visible if the configuration parameter QER\ComplianceCheck\CalculateRiskIndex is set. Refer to section Risk Evaluation on page 427 for more information.

- Category
  Categories are relevant for user accounts to inherit groups. User accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. Use the <Category> list to assign one or more categores to the user account. Define your categories in for the corresponding client (see Specifying Categories on page 354). The principle of inheritance is explained in detail in section Inheriting Group Memberships Based on Categories on page 82.

There are some user accounts that are added to the system during installation that are not assigned to a company. However, <Company> is a mandatory field. User accounts like this can still be loaded into

The Identity Manager during synchronization. In this case, they are assigned the default company name. Take note the following information for resynchronizing:.

- <Company> is a mandatory field!
- Changes to user accounts that are not assigned a company in the system cannot be saved in the Identity Manager by synchronization (without change data).
- Assign these user accounts a default company in the system where possible.

User Account Login Data

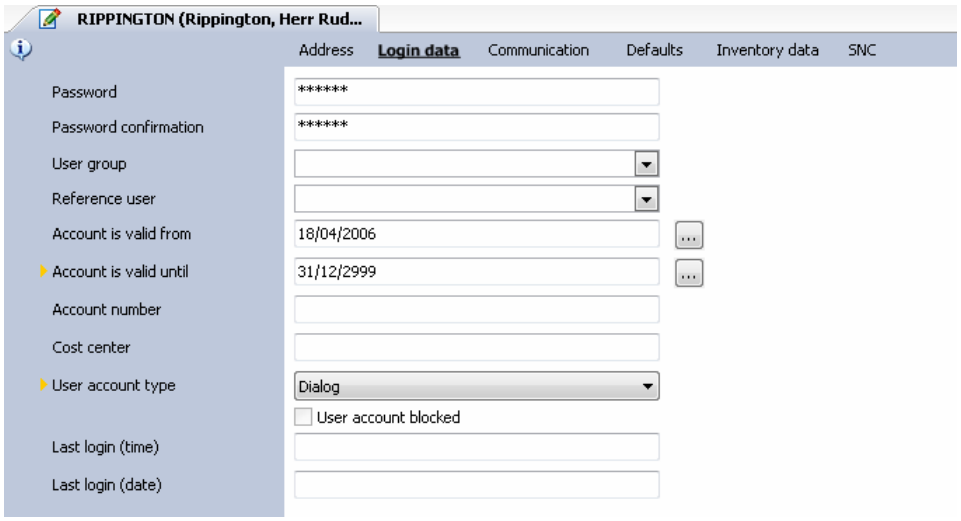
Configuration Parameter for Setting Up a User Account

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\UserDefaults\InitialPassword	Preset initial password for new user accounts. Note the minimum password length for the initial password! It can be a maximum of 14 characters. The password needs to be encrypted!
TargetSystem\SAPR3\UserDefaults\InitialRandomPassword	A random generated password is generated when a new user account is added. It must contain at least those character classes that are set in the child configuration parameters.
TargetSystem\SAPR3\UserDefaults\Ustyp	Specifies the default user type for user accounts.
QER\Person\UseCentralPassword	The employee's central password is automatically mapped to the employee's user account in all permitted target systems.

When a user account is added, you issue them it a password. Once you have saved the user account password with the Identity Manager it cannot be changed. You can set an initial password for newly added user accounts with the configuration parameter "TargetSystem\SAPR3\UserDefaults\InitialPassword". Use the parameter "TargetSystem\SAPR3\UserDefaults\InitialRandomPassword" to specify whether a randomly generated password should be issued to a new user account. The child parameters specify the character sets that the password needs to contain and the email address that the password

should be sent to. Depending on the configuration parameter "QER\Person\UseCentralPassword", the employee's main password can be mapped from the user account password.

User Account - Login Data



Enter the following login data for a user account:

- Password, password confirmation
  Password for a new user account.
  Changes to these input fields for existing user accounts can not be saved.

- User group
  Assign a group that provides the user account with defined authorizations.

- Reference user
  Assign a reference user whose authorizations are passed onto the user account.
  A reference user is a user account with the user type "reference". Use reference users to supply identical authorizations to different user accounts within one client.

- Account valid from, account valid til
  Validity period for this user account.

- Account number, cost center
  You can assign a cost center and a account number to the user account for accounting purposes.

- User type
  Select a user type from the list.
  The default user type is defined in the configuration parameter "TargetSystem\SAPR3\UserDefaults\Ustyp". Refer to section User Account Types on page 362 for an explanation of each user type.

- User account blocked
  This option is set if the user account has been locked by the task <Lock account>. An employee cannot log onto an system with this user account. Use the <Unlock account> task to allow this user account access to the system again.
  If the user account is linked to an employee, the behavior can be controlled by disabling or deleting the employee. Refer to the section Handling Disabling and Deletion of Employees and User Accounts on page 44.

- Last Login
  The date and time of the last login are read from the SAP R/3 environment and cannot be changed.

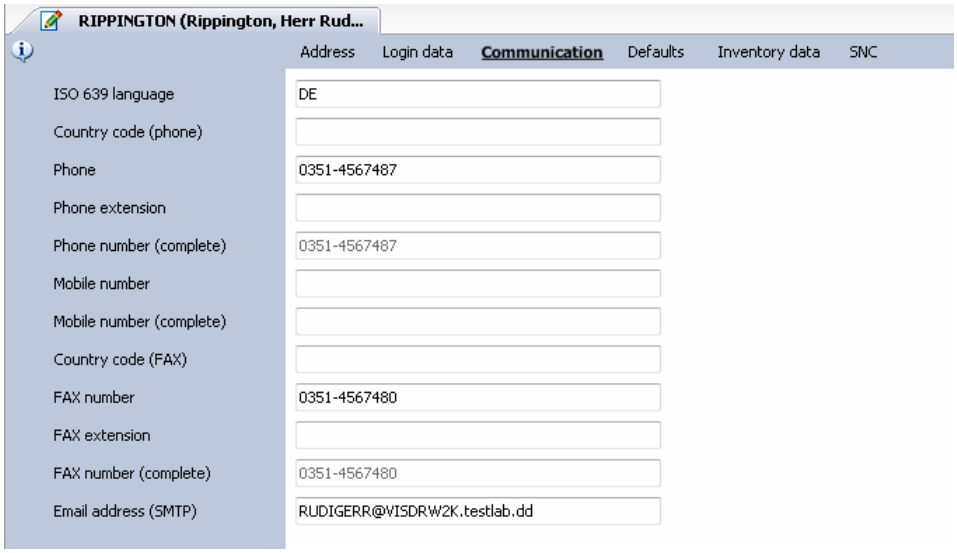
Contact Data for a User Account

Configuration Parameter for User Account Setting

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\UserDefaults\Langu_p	Specifies default language key for SAP R/3 users.
TargetSystem\SAPR3\UserDefaults\Langup_iso	Specifies default language (ISO 639).

Enter information for contacting the user on the <Communication> tab. This includes telephone and fax numbers as well as email. The language key is determined by the configuration parameter "ameSpace\SAPR3\UserDefaults\Langu_p".

User Account - Communication Data



Fixed Values for a User Account

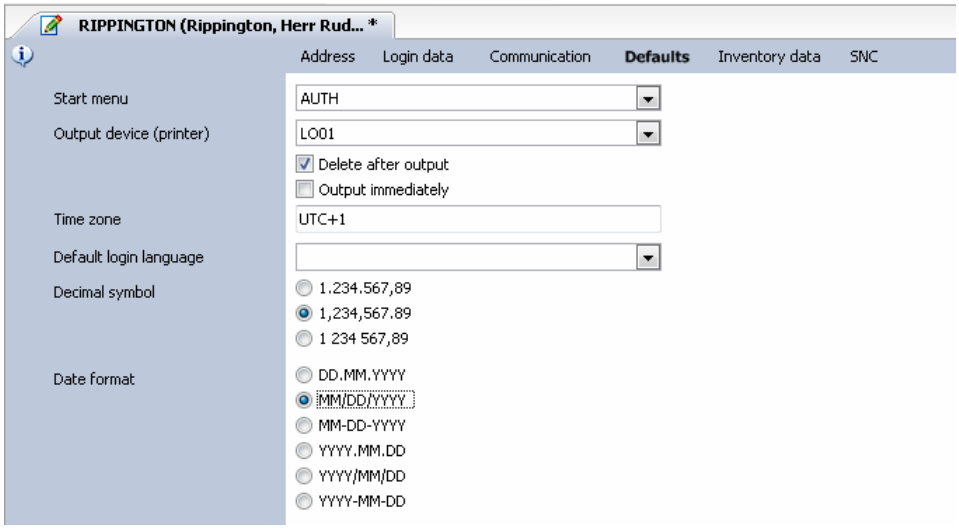
Configuration Parameter for User Account Settings

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\UserDefaults\Datfm	Specifies the default date format for user accounts.
TargetSystem\SAPR3\UserDefaults\Dcpfm	Specifies the default decimal point format for user accounts.
TargetSystem\SAPR3\UserDefaults\Fax_Group	Specifies the default fax group for user accounts.
TargetSystem\SAPR3\UserDefaults\Guiflag	Specifies whether secure communication is permitted for user accounts.
TargetSystem\SAPR3\UserDefaults\Spda	Specifies default setting for printer parameter 3 (delete after print).
TargetSystem\SAPR3\UserDefaults\Spdb	Specifies default setting for printer parameter 3 (print immediately).
TargetSystem\SAPR3\UserDefaults\Splg	Specifies the default printer (print parameter 1).
TargetSystem\SAPR3\UserDefaults\Time_zone	Specifies the default time zone value for the user account's address.
TargetSystem\SAPR3\UserDefaults\Tzone	Specifies the default value for the time zone.

Enter the default values that are to be put into effect for the user account on the <Defaults> tab. This includes data such as the start menu, which should be shown after login, the default login language, personal time zone, decimal representation or date format that the user is going to work with.

In addition, specify the spooling data such as output device and the spool options. The values for defaults are partially provided by the configuration parameters.

User Account - Default Values



Inventory Data

The license data for system measurement are shown here. This topic is gone into in detail in the section Providing System Measurement Data on page 394.

SNC Data for a user account

Enter the user account SNC name in the input field <SNC name> to log into the system over Secure Network Communications (SNC). You can find the syntax for SNC names in the SNC user manual.

System Assignment for CUA

Assign the CUA client system to the selected user where the user will be given login permissions. The tab <System> is only displayed if the selected user's client is labeled as central system.

Additional Tasks for Managing user accounts

After you have entered the user account master data, you can apply different tasks to it. You can see the most important information about the user account on the overview form. The task view contains different forms with which you can run the following tasks.

Assign Extended Properties

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Extended properties are meta objects that are not directly mapped in the Identity Manager data model, such as accounting codes, controlling areas or cost accounting areas. Extended properties are used for checking conformity to rules. You can find more information in section Setting Up Extended Properties on page 424.

Assign Groups, Roles, Profiles and Structural Profiles

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

All groups, roles and profiles for a usr are shown on the overview form. Groups (roles, profiles and structural profiles) can be assigned directly or indirectly to a user account. Indirect assignment is done by assigning an employee and the group (roles, profiles, structural profiles) to roles. If the employee has a user account it inherits the groups (roles, profiles, structural profiles) in this role. You can also assign the groups (roles, profiles, structural profiles) directly to a user account in order to respond quickly to special demands. Use the forms <Assign groups>, <Assign roles> and <Assign profiles> and <Assign structural profiles> to do this. You can find more information in section Assigning Company Resources through Roles on page 78.

Only profiles that are NOT profiles generated from an role can be directly assigned to user accounts.

Remember to take in to account the behavior of the SAP synchronizer described in section Special Assignment Cases for User Accounts and Groups, Profiles and Roles on page 387 when you are assigning groups, roles and profiles.

Lock Account

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

If you run the task <Lock account> on a user account the user can no longer login with this user account onto an system. The moment the DBScheduler has processed the task queue, the option <Unlock account> appears on the master data form on the <Login data> tab. Use the task <Unlock account> to allow this user account to log onto the system again.

If the user account is linked to an employee, the behavior can be controlled by disabling or deleting the employee. Refer to the section Handling Disabling and Deletion of Employees and User Accounts on page 44.

Managing user accounts with User Account Resources

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

You can automatically create user accounts for company employees with the help of user account resources. You can set up user account resources for any domain in an SAP environment. The basic mechanisms are explained in the section Creating User Accounts with User Account Resources on page 37.

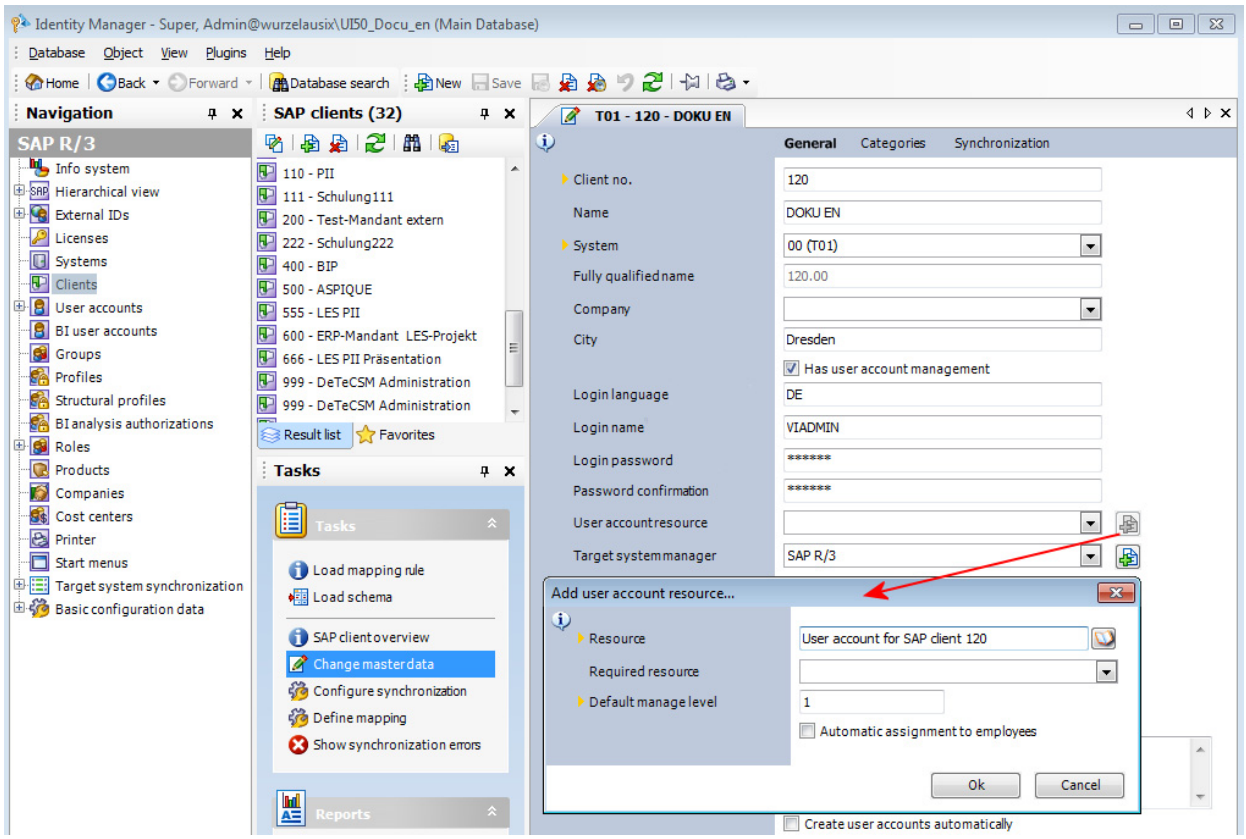
Should an employee get a user account through user account resources, he or she must have a central user account.

When a user account resource is assigned to an employee, a check is made to see if a user account already exists in the user account resource domain. If there is no user account, a new user account is created with the user account resource default manage level. If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

Creating a User Account Resource for an Client

You can set up a user account resource for an client in the category <SAP R/3>\<Clients>. Enter the data for the new user account resource by clicking on the button next to the input field on the master data form.

Creating a User Account Resource for an Client

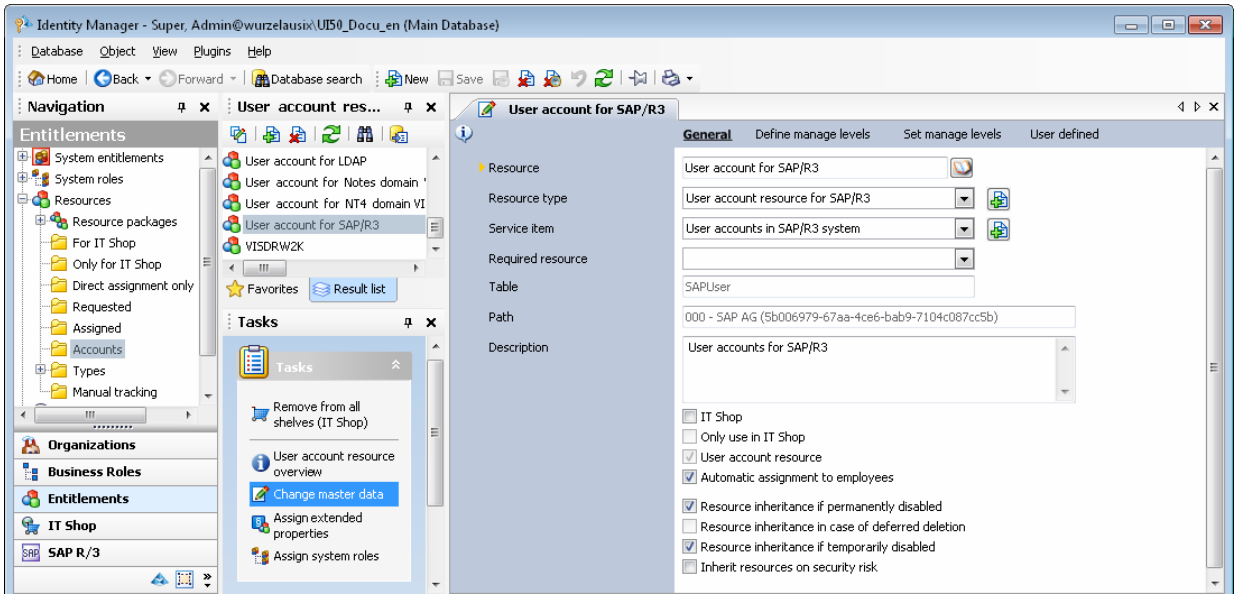


Enter the following data for the user account resources:

- Resource identifier
- Default manage level
  Specify the default manage level to be used when user accounts are added using this user account resource. To create user accounts in the Identity Manager default installation with a manage level ”Full Managed“ enter the value ”1“ here. User accounts with an manage level ”Unmanaged“ are created if the default level is ”0“.
- Assumed resource
  This field defines a dependency between user account resources. Leave this field empty for clients.
- Automatic assignment to employees
  Label the user account resource with this option when it should be automatically assigned to all internal employees. On saving, the user account is assigned to every employee not marked as external. The moment a new employee is added, they also are assigned this user account.The assignment is computed by the DBScheduler.

A new user account resource is created when the data is saved. You can subsequently edit the other data for this user account resource in Identity Manager in the category <Entitlements>\<Resources> in the filter <Accounts> and in the Manager in the category <Resource & Groups>\<Resources> in the filter <Accounts>.

Reworking the User Account Resource



Additional data for user account resources is:

- Resource type
  Resources should obtain a resource type. This resource type defines future post-processing steps for resource requests or resource assignments. You can add a new resource type using the button next to the input field.
  If you are working with the Identity Manager add new resource type using a user account with the application role <IT Shop>\<Administrators> in the category <Entitlements>\<Basic configuration data>\<Resource types>.

- Service item
  Assign a <service item> to the user account resource or add a new one. This means that the user account resource can be requested through the IT Shop.
  If you are working with the Identity Manager add new resource type using a user account with the application role <IT Shop>\<Administrators> in the category <IT Shop>\<Service catalog>\<Requestable service items>.

- Table
  Base table in which the user account is displayed.
  This input is preset with the value ”SAPUser“ when the user account resource is assigned to an client and cannot be changed.

- Path
  The path used by the user account resources.
  This input is preset with the NetBIOS name of the client when the user account resource is assigned to an client and cannot be changed.

- Description
  An empty text field for your own information about the user account resource.

- Data for use in IT Shop
  Mark a user account resource with the option <IT Shop> if it is going to be requestable in the IT Shop. These user account resources can be requested by the employees over a web front-end and distributed with a defined approval policy. The user account resource can still, however, be assigned directly to an employee and non-IT Shop roles. In order to avoid direct assignment, activate the option <Only use in IT Shop>. In this case user account resources can only be requested through the IT Shop.

- User account resource
  Labels the selected resource as a user account resource. This option can not be edited.

- Resource inheritance
  You define the inheritance behavior of the user account resource yourself. The inheritance options of the previous resources are overwritten. This resource inheritance behavior may be desired in order to, for example, ensure that all required permissions are immediately reinstated for an employee that is reactivated at a later date. You can activate the following options for resource inheritance...:

...if permanently disabled	Option set: if an employee is disabled permanently, the user account resource remains assigned to the employee. The user account is disabled. Option not set: the user account resource is no longer inherited by the employee. The associated user account is deleted.
...in case of deferred deletion	Option not set: if an employee is marked for deletion, the user account resource assignment to the employee is deleted. The associated user account is deleted. This option cannot be set.
...if resource inheritance temporarily disabled	Option set: if an employee is temporarily disabled the user account resource remains assigned to the employee. This user account is disabled. Option not set: this user account resource is no longer inherited by the employee. The associated user account is deleted.
...on security risk	Option set: if an employee is rated as a security risk, the user account resource remain assigned to the employee. he associated user account is disabled. Option not set: the user account resource assignment to the employee is deleted. The associated user account id deleted.

Specifying Manage Levels for Handling User Accounts

You can specify the manage level for a user account resource for handling user accounts. The manage level determines the scope of the properties that a user account inherits from an employee.

Therefore, an employee can, for example, have several user accounts in one client:

- A default user account that inherits all properties through the employee

- Administrator user account that although linked to the employee, should not inherit any properties.

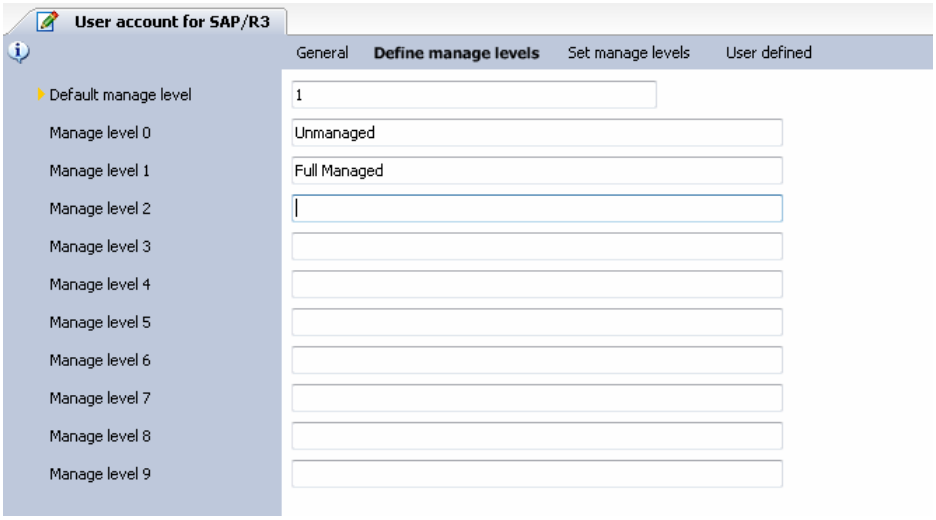
The Identity Manager’s default installation is configured for the manage levels ”Unmanaged“ and ”Full managed“. User accounts with the manage level ”Unmanaged“ are merely linked to an employee but do not inherit other properties. User accounts with the manage level ”Full managed“ inherit defined emplo-

yee properties. You can define other manage levels depending on the company's requirements. Then you need to extend your templates to include the methods for the addition manage levels.

When a user account resource is assigned to an employee, the default manage level of the user account resource is used to create the user account. If more clients should be managed using user account resources, you have to create a separate user account resource per client. Each user account resource has to use a different default manage level. This behavior is a custom setup and is not implemented by default. There is an example in section Creating User Accounts with User Account Resources on page 37 which explains this in more detail.

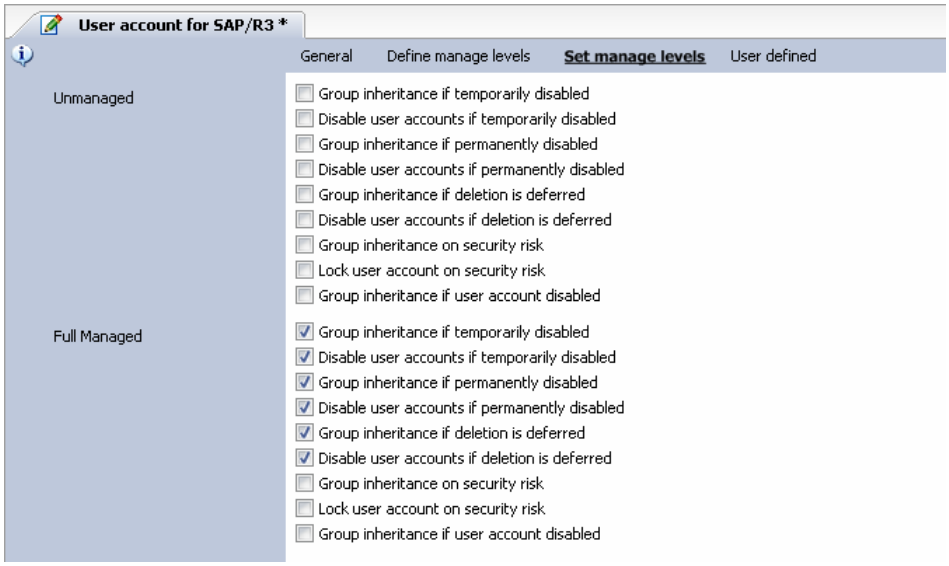
Define manage levels on the master data form for the user account resource on the <Define manage level> tab (Identity Manager: category <Entitlements>\<Resources>, filter <accounts>; Manager: category <Resources & Groups>\<Resources, filter <accounts>).

Manage Levels for a Client User Account Resource



On the <Set manage levels> tab, specify the effects of temporary or permanent disabling, deletion and security risk on an employee's user accounts and group memberships.

Editing User Account Resource Manage Levels


User account for SAP/R3 *
General
Define manage levels
Set manage levels
User defined
Unmanaged
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled
Full Managed
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled

user accounts can be locked when the employee is disabled, deleted or rated as a security risk so that authorizations are immediately withdrawn. If an employee is re-enabled at a later date, the user accounts can also be reactivated. This behavior is controlled by the properties:

- Disable user accounts if permanently disabled
- Disable user accounts if temporarily disabled
- Disable user accounts if deletion is delayed
- Disable user accounts if security is at risk

Group membership inheritance can be defined for a user account resource for an area of a target system. Inheritance may be discontinued if the employee's user account is locked and therefore may not become a member in a global group. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted! This behavior is controlled by the properties:

- Group inheritance if permanently disabled
- Group inheritance if temporarily disabled
- Group inheritance if deletion is delayed
- Group inheritance if security is at risk

You can find further information in the section Handling Disabling and Deletion of Employees and User Accounts on page 44.

Deleting User Account Resources

Tool: Manager

You can delete user account resource if they are no longer assigned to an client or any employee or role. Proceed as follows:

1. Select category <Resources & Groups>\<Resources>\<Accounts>
2. Remove user account resource assignments to employees and roles
3. Select category <SAP R/3>\<Clients>
4. Remove user account resource assignments to clients
5. Select category <Resources & Groups>\<Resources>\<Accounts>
6. Select the user account resource in the result list and delete it

Deleting user accounts

Configuration Parameters when Deleting User Accounts

CONFIGURATION PARAMETER	EFFECT WHEN SET
QER\Person\User\DeleteDelay	Delay on deletion

You can delete a user account from the result list or the menu bar. After confirming the deletion prompt, the user account is marked for deletion in the Identity Manager and access to the system is no longer permitted. The user account is deleted from the client and the Identity Manager database depending on the setting of the configuration parameters "QER\Person\User\DeleteDelay ". During this time it is possible, using the context menu entry <Reset delete>, to reset the status to "changed". The configuration parameter has no influence over the login permission in assigned CUA client systems.

Automatically Adding and Deleting user accounts by Changing Group Memberships

Configuration Parameters when Changing Group Memberships

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\PersonInheriteSAPGroup	Preprocessor relevant configuration parameter for passing on groups, profiles and roles to employee. Inheritance is recalculated when modifications are made to the configuration parameter. Changes to the parameter require recompiling the database.

You can assign groups, profiles and roles not only to user accounts in the Identity Manager but also to employees. The Identity Manager ensures that the required group memberships are created for the employee's user account.

Assign an employee groups (profiles, roles) in an client in which the employee does not yet have a user account. Then the Identity Manager can automatically add a new user account in this client and create the group memberships. If an employee in an client is no longer assigned to a group (profile, role), the Identity Manager ensures that the employee's user account is automatically deleted in this client.

To use this method, the following prerequisites need to be fulfilled:

- Configuration parameter "TargetSystem\SAPR3\PersonInheriteSAPGroup" is enabled.
  You can only assign groups, profiles or roles to an employee if this parameter is set. If you disable the parameter at a later date, it prevents assignment of group, profiles and roles to the employee. However, the groups memberships for the employee's user accounts remain intact.
- The employee requires a central user account. The user account name created in clients is taken from the central user account.
- The client has a user account resource.
- If user account should be created automatically, you must enable the option <Create user automatically> in the clients.
- If user account should be deleted automatically, you must enable the option <Delete user automatically> in the clients.

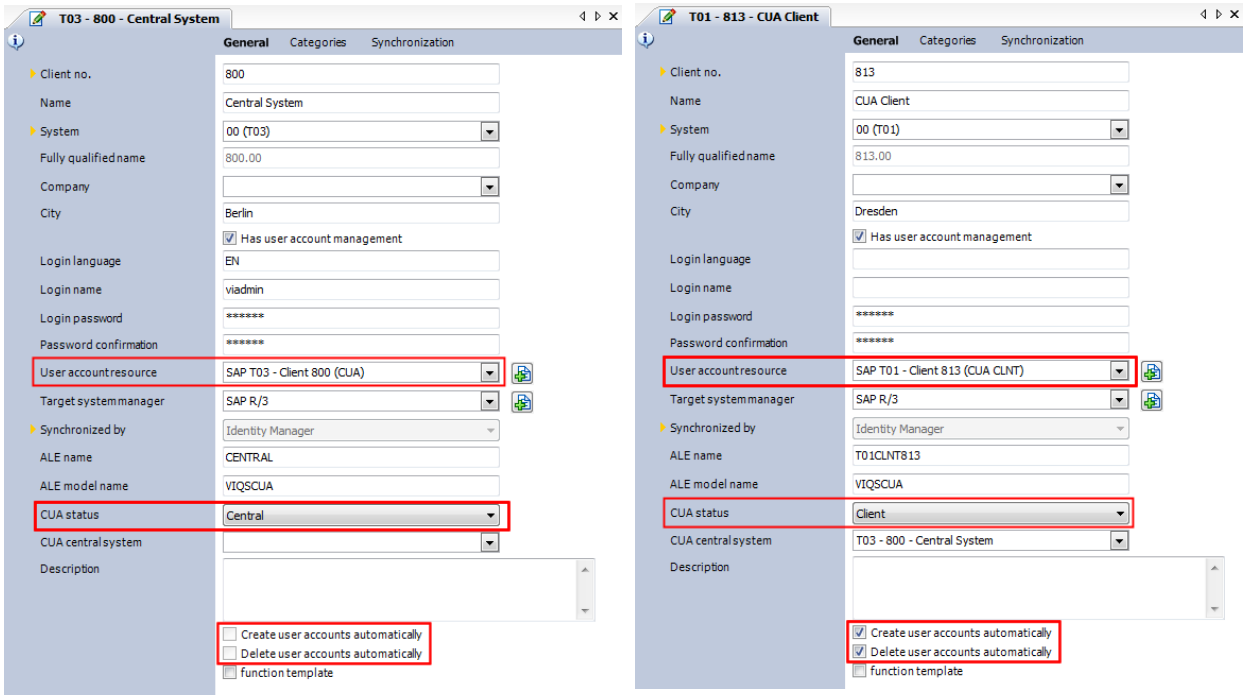
These functions are recommended when an employee is assigned products or they can be requested through the Identity Manager web front-end. Refer to section Compiling Products on page 390.

If an employee is assigned the client's user account resource and the option <Delete user automatically> is set, the employee must also be assigned a group or will be. Otherwise the employee's user account resource is removed (because of the option <Delete user automatically>).

CUA Implementation Features

If you use this functionality for controlling a Central User Administration, ensure that all client system user account resources have a required resource assigned to them. The required resouce must also be the user account resource of the associated central system.

Assigning User Account Resources to Central and Client Systems

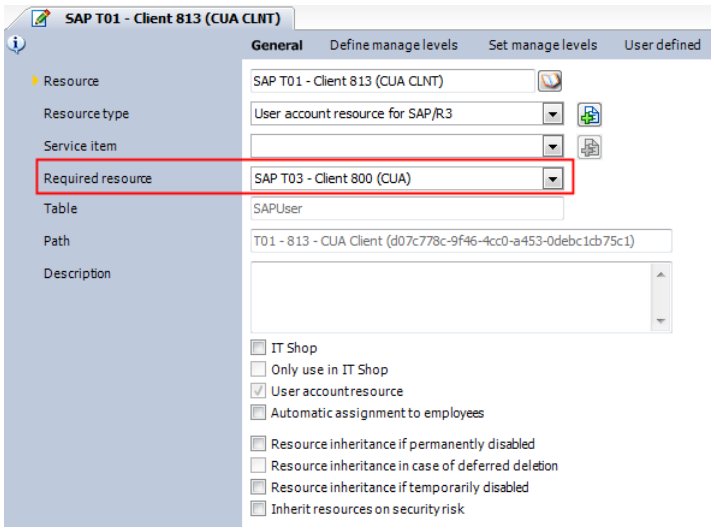


The options <Create user automatically> and <Delete user automatically> must not be enabled on the central system!

Specify the dependencies between user account resources in Identity Manager in the category <Entitlements>\<Resources>\<Accounts>. You can also define dependencies in Manager in the category <Resources & Groups>\<Resources>\<Accounts>. To do this, open the master data form for the client

system user account resource and assign to it the central system user account resource in the input field <Required resource>.

Specifying Dependencies Between User Account Resources



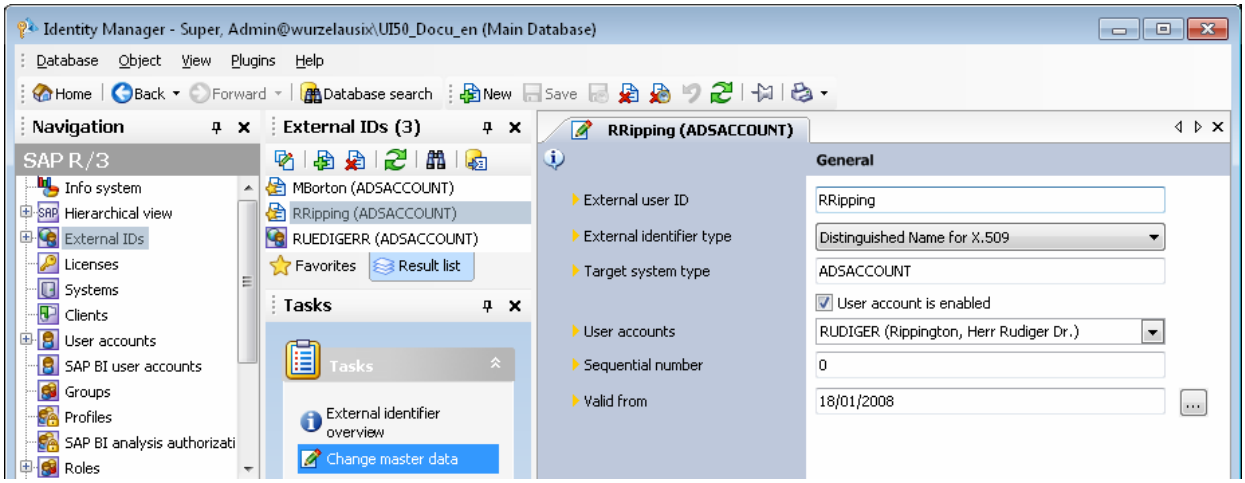
Entering External User Identifiers for a User Account

Configuration Parameter for External User Identifiers

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\UserDefaults\ExtID	Specifies default user type for external identification of SAP R/3 users
TargetSystem\SAPR3\UserDefaults\TargetSystemKennung	Specifies default target system ID for representing external users.

The Identity Manager allows maintenance of login data for logging external system users into an system for example Active Directory or Windows NT. Edit external users in the category <SAP R/3>\<External IDs>.

User Account External ID Input



Enter the following data to set up an external user ID:

- External user ID
  Enter the login name that the user logs in with on the external system. The syntax depends on the selected authentication method.

- External ID type
  Select the authentication type for the external user here. The syntax for the external ID results from this. Permitted are the values:

DN	Login using the Distinguished Name for X.509
NT	Login using Windows NT Lan Manager or password verification with the Windows domain controler
LD	Login using LDAP Bind (for other external authenication mechanisms)

- Target system type (ADSAccount or NTAccount)
  This input, together with the external ID type, can be called up to test the login data in the Identity Manager.

- Account is enabled
  If this option is set, the user can log into the system using an external authentication system.

- User accounts
  Enabling the external user ID

- Sequential number
  If a user account has several external IDs, label them with a squential number.

- Valid from
  Date fromwhich the external user ID is valid

Groups, Profiles and Roles Administration

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Configuration Parameter for Groups, Profiles and Roles

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\SAPR3\RedoDelay	This configuration parameter specifies the delay time after which an incompleted update is repeated. The input is in minutes.

In order to provide the necessary permissions for user accounts, groups, roles and profiles are mapped in the Identity Manager. The groups, roles and profiles are load into the data during synchronization. There is only a limited amount of editing you can do to these objects in the Identity Manager. No new groups, roles or profiles can be added or deleted.

You can share maintainance of user accounts over different administrators by assigning user accounts to groups. Groups are displayed in the Manager in the category <SAP R/3>\<Groups>.

An SAP role includes all transactions and user menus that one SAP user requires to fulfill its tasks. Roles are separated into single and collective roles. Single roles can be group together into collective roles.

User member in the roles can be set for a limit period. Roles are displayed in the Manager in the category <SAP R/3>\<Roles>.

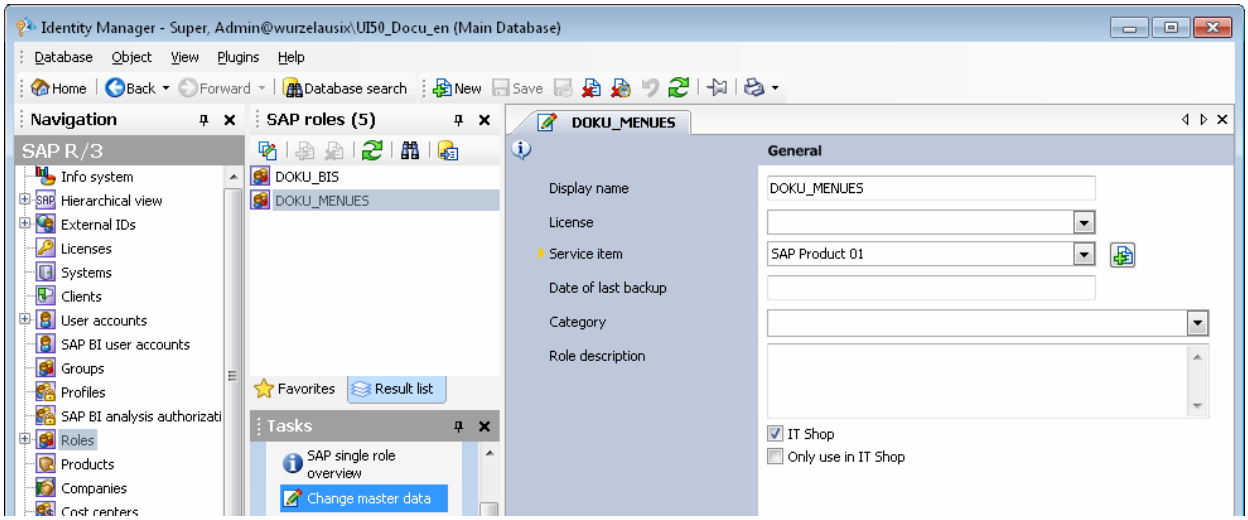
Access permissions to the system are regulated though profiles. Profiles as assigned through roles or directly to user accounts. Profiles are displayed in the Manager in the category <SAP R/3>\<Profiles>.

You can edit the following data for groups, roles and profiles in the Identity Manager:

- License information for system measurement
- IT Shop usage
- Risk assessment
- Inheritance restriction
- Name and description used for displaying in the Identity Manager
- Assigned user accounts
- Assigned roles

Other object properties cannot be edited.

Example of a Role



Edit the following master data for a group (role, profile):

- Display name
  Name of the group (role, profile) for displaying in the Identity Manager tools. Is normally taken from the group (role, profile) name.

- License
  This input is necessary to determine the sz data for user accounts and is assigned once after synchronization. Permitted licenses are loaded during synchronization. You can find other information in the sections Licenses on page 363 and Providing System Measurement Data on page 394.

- Service item
  So that groups, roles and profiles can be requested through the IT Shop assign an service itemto them or add a new one.
  If you are working with the Identity Manager add new service item using a user account with the application role <IT Shop>\<Administrators>.

- Date of last backup
  Date of last object changes in the system.
  Is evaluated for speeding up synchronization. Refer to section How to Speed up Synchronization on page 174.

- Risk index
  Here you can enter a value for rating a group (roles, profiles) for assessing the risk of group (roles, profiles) assignments to user accounts in the context of Identity Audit. Enter a value between 0 and 1.
  This input field is only visible if the configuration parameter QER\ComplianceCheck\CalculateRiskIndex is set. Refer to section Risk Evaluation on page 427 for more information.

- Category
  Categories are relevant for user accounts to inherit groups (roles, profiles). User accounts can selectively inherit groups (roles, profiles).To do this, groups (roles, profiles) and user accounts are divided into categories. Use the <Category> list to assign one or more categores to the group (role, profile). Define your categories in for the corresponding client (see Specifying Categories on page 354). The principle of inheritance is explained in detail in section Inheriting Group Memberships Based on Categories on page 82.

- Description/role description
  Description of the group (profile)
  Description of the role for displaying the Identity Manager tools.

- Data for user in IT Shop
  Set the <IT Shop> option if the group (role, profile) can be requested through the IT Shop. Then the group (role, profile) can be requested from the IT Shop's employees and granted through a defined approval procedure. The group (role, profile) can still however be assigned directly to a user account. Set the option <Only for user in IT Shop> to prevent direct assignment. In this case the group can only be requested through the IT Shop.
  If you set this option, assign a service item to the group (role, profile). This allows the group (role, profile) to be added to the IT Shop.

Additional Tasks for Managing Groups

After you have entered the master data, you can apply different tasks to the permissions. You can see the most important information about groups, roles and profiles on the overview form. The task view contains different forms with which you can run the following tasks.

Assign Business Roles and Organizations

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

It is possible for user accounts to inherit these permissions if groups, roles and profiles are assigned to individual company structures. Use the task <Assign business roles and organizations> to assign groups, roles and profiles to departments, cost centers, locations or business roles. If an employee is added to one of these company structures and this employee has user accounts then this employee is given the groups, roles and profiles. You can find further information in the section Assigning Company Resources through Roles on page 78. If an employee does not have a user account, one can be created by following the conditions described in the section Automatically Adding and Deleting user accounts by

Changing Group Memberships on page 380 and therefore provided with the necessary group memberships.

Inheritance procedures are calculated by the DBScheduler. Restrictions on the SAP side that apply in this case and their effect on assignments and the inheritance behavior in the Identity Manager, are explained in more detail in the sections Inheriting SAP System Authorizations and SAP Products on page 295 and Features for Assignment and Inheritance of SAP Profiles and SAP roles to SAP User Accounts on page 299 in the Configuration Manual.

Adding to the IT Shop

Tools: Manager

When groups, roles and profiles are assigned to an IT Shop shelf the groups can be requested by the shop's customers. To ensure the groups, roles and profiles are requestable, further prerequisites need to be guaranteed. There is more information about this in the section Requestable Products on page 33. To remove groups, roles and profiles from the IT Shop, use the task <Remove from all shelves (IT Shop)>.

Assign user accounts

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Use the form <Assign user accounts> to directly assign groups, roles and profiles directly to user accounts.

Assign System Roles

Tools: Manager

Groups, roles and profiles can be added to different system roles. System roles that exclusively contain groups, roles or profiles can be labeled with the system role type "SAP product". You can find other information about SAP products in the section Compiling Products on page 390. Groups, roles and profiles can also be added to system roles that are not SAP products.

Specify Inheritance Exclusion

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Use the form <Specify inheritance exclusion> to define dependencies between groups, roles and profiles. By defining dependencies between the groups, the number of resulting memberships of user accounts is reduced in the groups, roles and profiles. Read more in section Inheritance Exclusion on page 80.

Assign Extended Properties for Groups, Roles and Profiles

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Extended properties are meta objects for which there is no direct mapping, such as accounting codes, controlling areas or cost center areas, in the Identity Manager data model. These extended properties are used to check rule conformity. For more information see section Setting Up Extended Properties on page 424.

Show Authorizations and Authorization Objects

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Authorizations and authorization objects for roles and profiles are read from the system during synchronization and cannot be edited in the Identity Manager. You can view the asssignments on the forms <Show SAP authorizations> and <Show authorization objects>. Synchronize the following object types and assignments in order to display authorization objects and authorizations on the forms:

Object Type	Assignment
TOBJ	SAPAUTHOBJECTOBJCT
TACT	SAPAUTHOBJECTFIELD
AUTHX	SAPGROUPAUTH
USVART	
TOBJ	
AUTH	

Special Assignment Cases for User Accounts and Groups, Profiles and Roles

The SAP synchronizer takes the configuration parameters "TargetSystem\SAPR3\SyncBehavior\ClearMembershipListOnChange" and "TargetSystem\SAPR3\SyncBehavior\SyncValidRolesOnly" into account when assigning and synchronizing group memberships with the user account.

If the configuration parameter "TargetSystem\SAPR3\SyncBehavior\ClearMembershipListOnChange" is enabled, any change that effects a user account's group, role or profile assignments causes the respective list to be completely deleted and recreated in SAP R/3. If the configuration parameter is not set, only entries that are directly effected are added or deleted when changes are made to a user account's group, role or profile assignments.

If the configuration parameter "TargetSystem\SAPR3\SyncBehavior\SyncValidRolesOnly" is set, only role assignments whose valid time period includes the current date are taken into account. This means that old assignments whose validity periods have been exceeded are not copied to the Identity Manager database. If this configuration parameter is not set, role assignments are not taken into account.

You can clean up the user account role assignment list by enabling both the configuration parameters.

Example:

The following roles are assigned to a user account in the SAP R/3 environment:

Assigned Roles

ROLE	VALID FROM	VALID UNTIL
Role01	01.01.2003	31.10.2004
Role01	15.06.2006	31.12.9999
Role02	01.01.2006	31.12.9999

Another role assignment "Role03" should be added.

If the configuration parameters "TargetSystem\SAPR3\SyncBehavior\ClearMembershipListOnChange" and "TargetSystem\SAPR3\SyncBehavior\SyncValidRolesOnly" are set, the following assignments are accepted as being valid:

Valid Assignments

ROLE	VALID FROM	VALID UNTIL
Role01	15.06.2006	31.12.9999
Role02	01.01.2006	31.12.9999

The role "Role03" is added to the list with the current date as 'valid from' date. The previous list is cleared in SAP and then reenabled. This results in the following role assignments:

Valid Assignments

ROLE	VALID FROM	VALID UNTIL
Role01	15.06.2006	31.12.9999
Role02	01.01.2006	31.12.9999
Role03	04.09.2006	31.12.9999

If the configuration parameters "TargetSystem\SAPR3\SyncBehavior\ClearMembershipListOnChange" and "ameSpace\SAPR3\SyncBehavior\SyncValidRolesOnly" are not set, the following role assignments are the result:

Valid Assignments

ROLE	VALID FROM	VALID UNTIL
Role01	01.01.2003	31.10.2004
Role01	15.06.2006	31.12.9999
Role02	01.01.2006	31.12.9999
Role03	04.09.2006	31.12.9999

You can delete old assignments that are already in the Identity Manager database using the scheduled task "Delete expired role assignments for SAPUSER". You can customize and run this task with the help of the Schedule Editor in Designer. Refer to the section Setting Up Scheduled Tasks on page 73 for more information.

Reports About System Entitlements

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

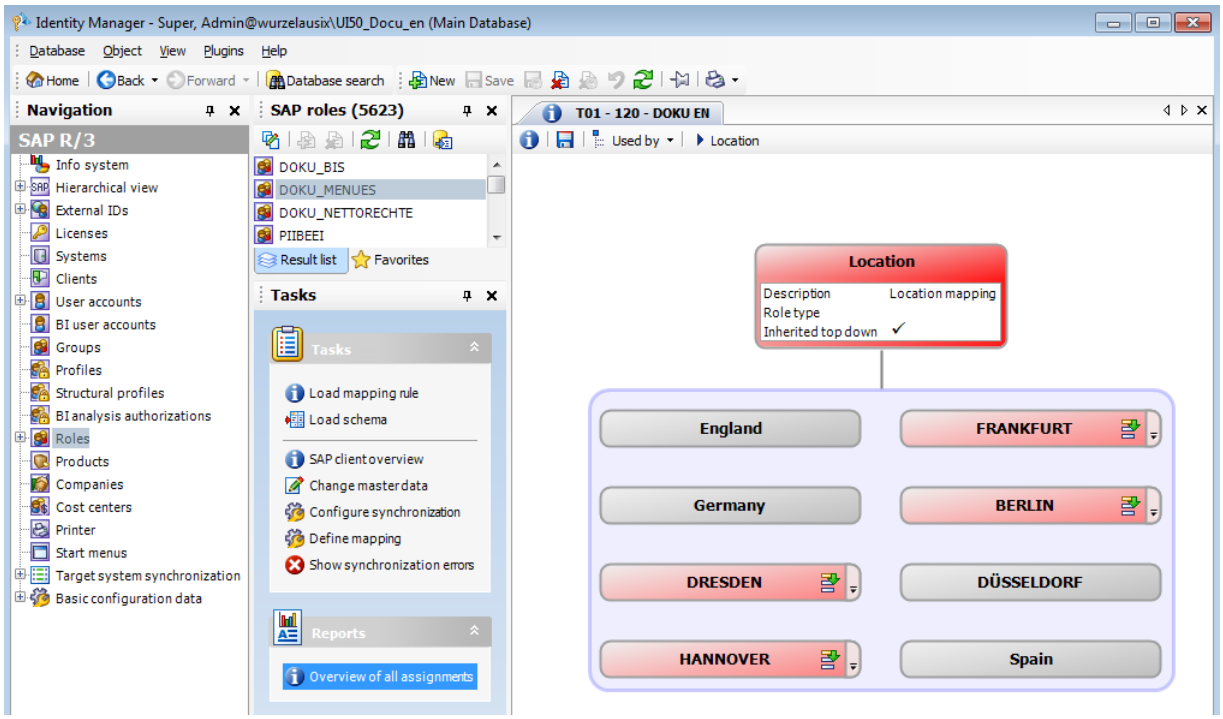
The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for groups, roles and profiles.

Overview of all Assignments

This report shows all employees that are assigned to at least one user account in the selected group (role, profile). Directly assigned objects as well as those object inherited by the employee are take into

account in this case. The report shows which roles of a role class the employee belongs to. What you get is an organigram of the different role classes for the selected group (role, profile).

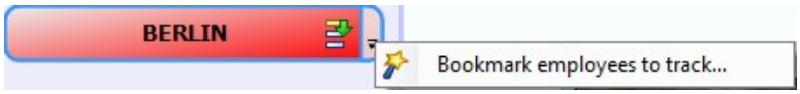
Report "Overview of all Assignments" for a Role



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that have a user account in the selected group (role, profile) and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

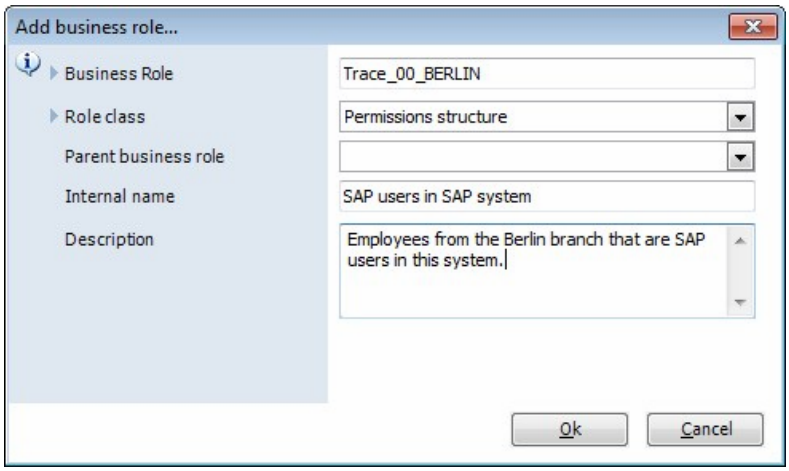
Bookmark Employee for Tracking



To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Compiling Products

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

You can define products as a group of different groups, roles or profiles. Products are system roles with the system role type ”SAP Product“. Employees can obtain products directly or inherit them through company structures. It is also possible to request products over the IT Shop. Groups, roles and profiles with the option <Only for use in IT Shop> can only be assigned to products that also have this option set. The employee’s user account is assigned the groups, roles and profiles in the product independent of the assignment method. If a product in the Identity Manager is modified by adding or deleting a group, profiles or a role, the user account group memberships are altered correspondingly. Please note the mechanisms described in the section Automatically Adding and Deleting user accounts by Changing Group Memberships on page 380.

Edit products in the category <SAP R/3>\<Products>. You also set up products in the Manager. Products are set up on the system role master data form. The system role type <SAP product> is already preset. Groups, roles and profiles can also be added to system roles that are not products. Refer to section Editing System roles on page 115 for more information.

Established inheritance mechanisms and calculation of product assignments by the DBScheduler is described in detail in the Configuration Manual in section Inheriting SAP System Authorizations and SAP Products on page 295.

Additional Tasks for Managing Products

After you have entered the master data for the product, you can apply different tasks to it. You can see the most important information about product on the overview form. The task view provides you with several forms that you can use to run the tasks described in the section Additional Tasks for Managing System Roles on page 116.

Managing Structural Profiles

Configuration Parameter for Structural Profiles

CONFIGURATION PARAMETER	MEANING WHEN SET
TargetSystem\SAPR3\HRProfile	Preprocessor relevant configuration parameter for controlling modules for structual profile administration (HR profiles) in SAP R/3. If the parameter is enabled the target system modules are available. Changes to this parameter require compiling the database. If this parameter is set these components are available in the target system.
QER\ComplianceCheck\CalculateRiskIndex	Preprocessor relevant configuration parameter for controlling calculation of an employee's risk index. Changes to this parameter require compiling the database. If this parameter is set, the values for the risk index can be entered and calculated.

The authorization concept for an system with an HR planning module is installed on top, provides another option for authorization checking. It is possible to define access to levels in personnel master data or the organigram that is related to concrete data in the HR module and if necessary can represent an access depth in terms of the organization tree. This access can also be bound to a deadline. These definitions are known as ”Structural profiles“ in the context of SAP.

Structural profile properties are displayed in the Identity Manager. Structural profiles can be assigned to a user account. Existing assignments to user accounts can be modified. Structural profiles can be requested through the IT Shop. This also makes it possible to assign structural profiles to user accounts for a limited period only. Structural profiles can be included in compliance checks.

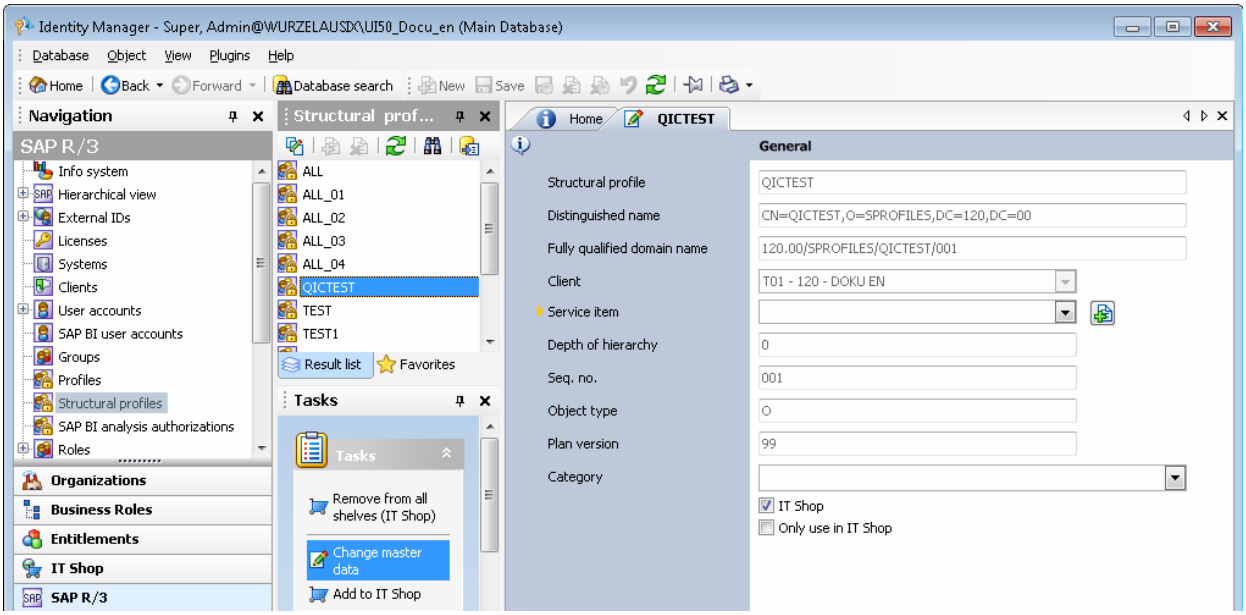
Set the configuation parameter ”TargetSystem\SAPR3\HRProfile“ so that structural profiles can be mapped in the Identity Manager. The configuration parameter is preprocessor relevant. Therefore, the database has to be compiled after changing the parameter. For more information about this, read section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual.

In order to edit structural profiles and their assignments to user accounts in the Identity Manager synchronize the following object types: USER, PROFILES.

Entering General Master Data for Structural Profiles

Tools: Identity Manager with application role <Target system>\<SAP R/3>; Manager

Edit structural profiles in the category <SAP3>\<Structural profiles>. Use the <Change master data> tab to enter the required data for a structural profile. Take care to fill out all the mandatory fields.



Editing Structural Profiles

Enter the following data for a structural profile:

- Structural profile
  Name of the structural profile.

- Distinguished name, fully qualified domain name
  The Distinguished name and the fully qualified domain name are formatted fromthe structural profile, client and system names using formatting rules.

- Client
  client that contains the structural profile.

- Service item
  Assign an existing service item to the structural profile so that it can be requested through the IT Shop or add a new service item.
  If you are working with the Identity Manager add new service item using a user account with the application role <IT Shop>\<Administrators>.

- Depth of hierarchy
  The number of the level in the hierarchy that the assigned user account is allowed to access down to.

- Seq. no.
  Sequential number of this structural profile.

- Object type
  The structural profile is valid for this object type.

- Plan version
  The structural profile is applied to this plan version.

- Risk index
  Here you can enter a value for rating a structural profile for assessing the risk of structural profile assignments to user accounts in the context of Identity Audit. Enter a value between 0 and 1.
  This input field is only visible if the configuration parameter QER\ComplianceCheck\CalculateRiskIndex is set. Refer to section Risk Evaluation on page 427 for more information.

- Category
  user accounts can selectively inherit structural profiles. To do this, structural profiles and user accounts are divided into categories. Use the <Category> list to assign one or more categores to the structural profile. Define your categories in for the corresponding client (see Specifying Categories on page 354). The principle of inheritance is explained in detail in section Inheriting Group Memberships Based on Categories on page 82.

- Data for user in IT Shop
  Set the <IT Shop> option if the structural profile can be requested through the IT Shop. Then the structural profile can be requested from the IT Shop's employees and granted through a defined approval procedure. The structural profile can still however be assigned directly to a user account. Set the option <Only for user in IT Shop> to prevent direct assignment. In this case the SAP can only be requested through the IT Shop.
  If you set this option, assign a service item to the structural profile. This allows the structural profile to be added to the IT Shop.

Additional Tasks for Structural Profiles

After you have entered the master data for the structural profile, you can apply different tasks to it. You can see the most important information about structural profile on the overview form. The task view provides you with several forms that you can use to run the tasks described in the following.

Assign Business Roles and Organizations

Tools: Identity Manager, Manager

It is possible for user accounts to inherit structural profiles when a structural profile is assigned to a role. The structural profile can be added to departments, cost centers, locations or business roles. Add an employee to this role and if the employee has a user account this user account obtains the structural profile. You can find further information in the section Assigning Company Resources through Roles on page 78.

Inheritance procedures are calculated by the DBScheduler. The principle of inheritance is described in section Inheriting SAP System Authorizations and SAP Products on page 295 in the Configuration Manual.

Add to IT Shop

Tools: Manager

When a structural profile is assigned to an IT Shop shelf is can be requested by customers of that shop. There are further prerequisites to fulfill to essure requestablibity of structural profiles. Refer to section Requestable Products on page 33 for more information. To remove a structural profile from all IT Shop shelves, run the task <Remove from all shelves (IT Shop)>.

Specify Inheritance Exclusion

Tools: Identity Manager, Manager

Use the <Specify inheritance exclusion> task to define dependencies between structural profiles. The number of resulting memberships of user accounts in structural profiles is limited by defining these dependencies. You can assign structural profiles that belong to the same client as the selected structural profile. For more information about dependencies between structural profiles see section Inheritance Exclusion on page 80.

Assign User Accounts

Tools: Identity Manager, Manager

Use this task to assign user accounts directly to the structural profile. You can assign user accounts that belong to the same client as the selected structural profile. All the user accounts that can be directly or indirectly assigned to the structural profile are displayed on the form. Edit direct user account assignments on this form. Change the assignment from employee or user account to roles to edit indirect assignments. For more information, refer to section Assigning Company Resources through Roles on page 78.

Providing System Measurement Data

An employee can have several user accounts which belong to different clients and systems. The most significant user account has to be found for the employee. The user account's significance is determined by the license that is assigned. The system measurement data is available in the Identity Manager, but the measurement itself takes place in the SAP R/3 environment.

In order to calculate the measurement data, you need to quarantee the following prerequisites:

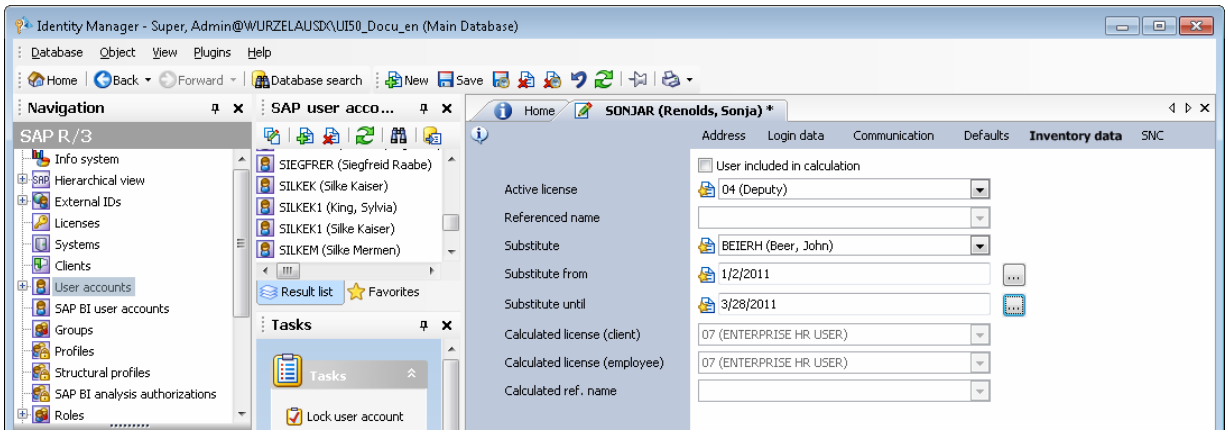
- The system must be labeled with the option <System measurement enabled> in the Identity Manager. Refer to section System Setup in the Identity Manager Database on page 349.
- The client must be set up for synchronization, that means the option <Has user account management> has to be set. Refer to section Client Synchronization Setup on page 352.
- The option <Synchronizes system measurement data (...)> has to be set in the synchronization configuration for the clients. Read section Special Features of Client Synchronization Configuration on page 358 for more information.
- The configuration parameter "TargetSystem\SAPR3\SyncObjects\SystemVermessung" is set.
- License entered for groups, roles and profiles. You need to make the assignment once manually after the objects have been synchronized! Read the sections Licenses on page 363 and Groups, Profiles and Roles Administration on page 383 for how license information is graphically represented.

Graphical Representation of Measurement Data

The measurement data is displayed on the user account's master data form on the <Measurement data> tab. Which fields are enabled on the form depends on the chosen license. If, for example, the license "04 (Deputy)" is selected for a user account, the input fields are enabled for assigning the deputy

user account and the deputizing validity period. If the license ”11 (Multi client/system user)“ is chosen, the list <Referenced name> is enabled.

Inventory Data



The following license information is displayed on the form:

- User included in calculation
  Set for the most highly rated employee of a user account.
  This option is set by the DBScheduler of the calculated licenses are published. For more information see section Transfering Calculated Licenses on page 398.

- Active License
  The active license corresponds to the user account license in the SAP R/3 environment. This license is loaded into the Identity Manager database by synchronization or determined from the calculated employee related licenses. For more information see section Transfering Calculated Licenses on page 398.
  The productive license is only synchronized when the option <Synchronize measurement data(...)> is set. For more detailed information see section Special Features of Client Synchronization Configuration on page 358.

- Reference name
  Link to the most significant user account if ”11 (Multi-client/system) is selected. Set by the Identity Manager.

- Substitute
  Link to the user account that deputizes for a specifed length of time. This input field is enabled if the active license is set to ”04 (substitute)“.
  The substituted user account obtains the authorizations in the system for the user account for this specify length of time.

- Substitute from/until
  Length of time that another user account is substitute. This input field is enabled if the active license is set to ”04 (substitute)“.

- Calculated license (client)
  The license that is determined from the group memberships within an client is entered for the user account.

- Calculated license (employee)
  The client related calculated license is entered for the most highly rated user account. For all the other employee's user accounts, the employee related calculated license "11 (Multi-client/system user)" is entered. These obtain an additional link to the calculated most significant user account which is entered under <Calculated ref. name>.

- Calculated ref. name
  Link to the calculated most significant user account if "11 (Multi-client/system user)" is entered. Set by the Identity Manager.

The procedure for determining the calculated licenses and the rating is described in section Determining User Account Rating on page 396.

Determining User Account Rating

A user account rating is determined in the Identity Manager through the rating of the groups, profiles and roles in which the user account is a member. The licenses have to be entered for the groups, profiles and roles as a prerequisite. You have to make this assignment once manually after the objects have been synchronized! When the most highly rated user account is determined, the license names and any manually issued license value is taken into account (see section Licenses on page 363).

In the following procedural description, groups, profiles and roles are combined together under the term "groups".

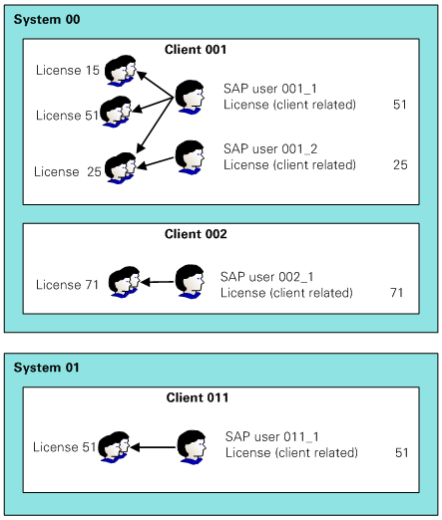
The most highly rated user account is determined in the Identity Manager in a two step process:

Determining the rating of the user account within an client (client related)
The group memberships within a client are calculated for a user account and the group with the highest rating is found. The license belonging to the group with the highest rating is copied to the user account. The most highly rated group fulfills the following crtieria:

6 a) The assigned license has the lowest license rating (in alphanumeric sort order).

6 b) The license with the highest ID is valid if several groups are assigned with the same license rating or no license rating is given.

Calculating a user account's Client Related Rating

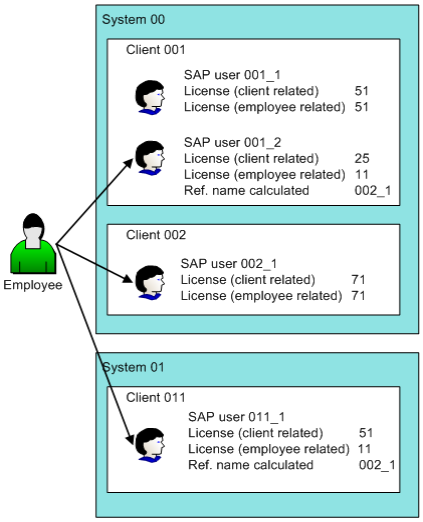


7. Determining the most highly rated user account (employee related)

7 a) The most highly rated user account is determined from all the employee's user account sin all clients and all systems. The criteria from 1a) and 1b) apply for these user accounts. The license for the most highly rated user account is assumed as the employee related license. For all other employee's user accounts, the license "11 (Multi-client/system user)" is entered. These user accounts are also given a reference to the most highly rated user account calculation.

7 b) If a user account is not assigned to an employee then the rating calculated in 1) is taken as the highest rating and the license is accepted.

Calculating the Employee Related Significance of a User Account

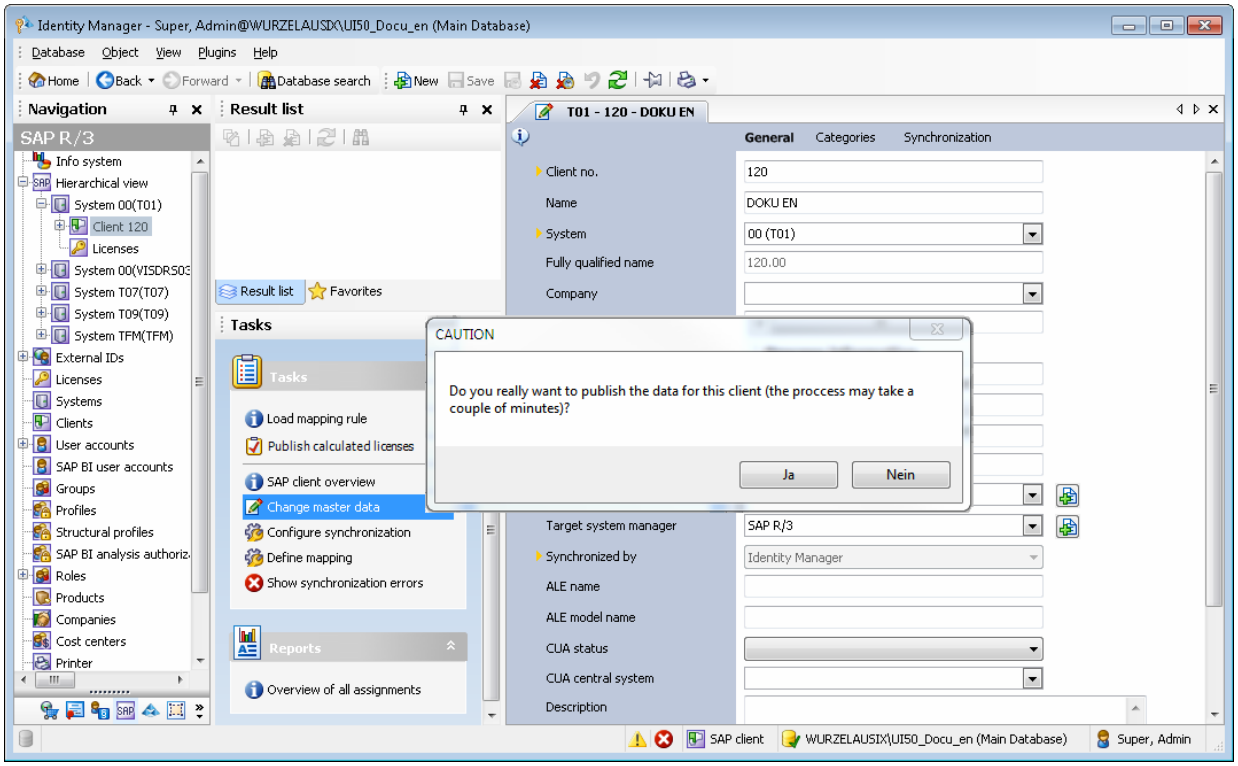


The DBScheduler executes the calculation of group memberships and determines the rating.

Transfering Calculated Licenses

In order to execute system measurement in the SAP R/3 environment, you need to transfer employee related calculated licenses to the active license. This transfer is done separately for each client in the system. Run the task <Publish calculated licenses>. You can manually rework the data if necessary.

Publishing Calculated Licenses



The Identity Manager transfers the calculated employee related license for all this client's user accounts to the active license. You can edit this data manually later if required (see section Graphical Representation of Measurement Data on page 394).

The option <User included in calculation> is set for the most highly rated user account of an employee. For all other user accounts of this employee, "11 (Multi-client/system)" is entered as the active license and a link is saved in the <Referenced name> list to the most highly rated user account.

12

Managing Generic Target Systems

- Introduction
- Special Cases for Implementing Synchronization between the Identity Manager Database and the LDAP Directory
- Setting Up LDAP Directory Synchronization
- LDAP Container Structures
- LDAP User Accounts
- LDAP Groups

Introduction

The Identity Manager allows administration of objects, such as employees, groups and organizational units that are managed in an LDAP directory. The LDAP structure in the Identity Manager has been developed from different LDAP schema. Core.schema, cosine.schema, inetorgperson.schema and openldap.schema were chosen as the underlying schemas. The properties required for employees and their user accounts are selected from these schemas. The LDAP structure in the Identity Manager should be seen as a suggestion and seldom corresponds to the property structure in a customer specific LDAP directory. Whether or how the available properties will be used depends on the respective LDAP schema which is in use and must be custom configured.

The default Identity Manager installation is concerned with employee administration and their user accounts, user groups and LDAP directory organizational units. The Identity Manager data model is designed to map LDAP locations as well as administration of LDAP directory computers and servers. However, the synchronization connection has to be custom configured in any case.

Company employees are provided with the necessary user accounts in the Identity Manager. Different mechanisms can be used to link employees to their user accounts. User accounts can also be managed separately from employees allowing administration user accounts (administrators) to be set up. In order to provide the required permissions, groups are managed in the Identity Manager. Furthermore, you can manage organizational units in a hierarchical structure. Organizational units (branches or departments) are used to logically organize the objects in an LDAP directory such as user accounts and groups and thus make administration easier.

Special Cases for Implementing Synchronization between the Identity Manager Database and the LDAP Directory

Identity Manager Service synchronizes objects between the Identity Manager and the LDAP directory. This is controlled by the process component ”LDAPADSIComponent“.

A mapping file (LDAPADSIComponent.dll.xml) is supplied for this process component, which contains extended rules for mapping properties between the Identity Manager and the LDAP directory. These mapping rules should be seen as a suggestion and seldom corresponds to the property structure in a customer specific LDAP directory. You need to check the process component formatting rules and if necessary change them before synchronization takes place with the LDAP directory and modify the mapping file if required.

Refer to the section Customizing Mapping rules on page 180 to find out how the mapping file is edited. The newly created mapping file must be stored in the Identity Manager Service installation directory on the synchronization server.

The processes contained in the default Identity Manager installation use the parameter mappings contained in the supplied mapping file in their process steps. The process steps and their parameters also have to be modified to fit the customer specific mappings. The process component has the user defined parameters ”Property1“ up to ”Property50“ to map the properties to the process functions ’Object Insert“ and ”Object Update“. To use these user defined parameters in the process steps, the parameter name is changed to the name of the column to be mapped (according to the property ”parametername“ on the data node in the mapping file) and the value template is modified.

Take note that it is not possible to customize Quest specific processes. Customer specific processes have to be created instead. The processes are edited in the Designer with the Process Editor. Read the section Defining Processes on page 46 on handling processes.

If the existing properties in the Identity Manager are not sufficient for representing the LDAP directory, you can use custom extensions of the Identity Manager data model to provide other properties. Use the

program Schema Extension to make the schema extension in the Identity Manager data model. Read the chapter Customer Specific Schema Extensions on page 343.

Setting Up LDAP Directory Synchronization

Identity Manager Service is responsible for comparing information between the LDAP directory. Synchronization prerequisites are:

- Installation and configuration of a synchronization server
- Database setup for synchronization

The basic synchronization mechanisms are explained in the chapter Data Synchronization in Identity Manager on page 161.

Installation and Configuration of the LDAP Synchronization Servers

To setup synchronization with an LDAP environment a server has to be available that has the following software installed on it:

Microsoft Windows Operating System

- Windows 2000 Server or Advanced Server with at least Service Pack 2 for Windows 2000, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 or Windows Server 2008 R2
- Microsoft .NET Framework at least version 3.5, service pack 1
- Microsoft Software Installation (MSI) service

Identity Manager Service is installed, configured and started on the synchronization server. The installation is described in the section Installing Identity Manager Tools on page 23. Pleas note the installation advice for Teminal Server installation (see Installing on a Microsoft Windows Terminal Server on page 25). Read the section Setting Up a Server for Database Access on page 44 for information about configuring Identity Manager Service.

The Identity Manager Database Setup for Synchronization with an LDAP Directory

Configuration Parameter for LDAP Directory Synchronisation

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\LDAP	LDAP is supported. Preprocessor relevant configuration parameter. The database has to be recompiled if the parameter is changed.
TargetSystem\LDAP\Accounts	Specifies use of user accounts.
TargetSystem\LDAP\Accounts\InitialRandomPassword	Preset password for adding user accounts.
TargetSystem\LDAP\MaxFullsyncDuration	Specifies maximum runtime for a synchronization.
TargetSystem\LDAP\PersonAutoFullSync	Depending on this parameter the decision is made as to whether automatic assignment of employee should come into effect when a user account is added during synchronization.
TargetSystem\LDAP\RedoDelay	This configuration parameter specifies the delay time after which an incompleted update is repeated. The input is in minutes.
TargetSystem\LDAP\RestoreMode	Determines the delta set resulting from sychronization of the Identity Manager database and the target system LDAP.
TargetSystem\LDAP\UseUSN	A comparison based on the modification date is performed when are LDAP objects are synchronized.
TargetSystem\LDAP\VerifyUpdates	Properties in the target system are tested by adding/inserting. The object properties are verified after each target system relevant process. This procedure can be used to rerun the process steps that write the properties in the target system. If the parameter is not set, testing does not take place.

Prerequisites for synchronizing the Identity Manager database with a LDAP directory:

- Necessary parameters must be changed and enabled.
  The configuration parameter ”TargetSystem\LDAP“ is a preprocessor relevant configuration parameter. This means that the database has to be compiled after changing this parameter. For more information read the section Compiling an Identity Manager Database on page 100 in the Getting Started Manual and Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual.

- Declare the synchronization server
  Refer to section Declaring the LDAP Synchronization Server on page 403.

- Declare the server that stores the LDAP Store
  Refer to section Declaring the LDAP Store Server on page 403.

- Declare the domain to be synchronized in the Identity Manager
  Refer to section Setting Up an LDAP Domain on page 403.

- Configure and enable scheduled tasks .

Declaring the LDAP Synchronization Server

Tools: Manager; Identity Manager with the application role <Target system>\<Generic target system>

All Identity Manager Service target system specific actions are executed by the synchronization server. Entries necessary for administration and synchronization with the Identity Manager database are processed by the synchronization server.

Configure new synchronization servers in the category <Generic target system>\<Basic configuration data>\<Server>. Enter a minimum of the following data for the synchronization server:

- Server
  Server name
  The server name is used to compose the queue name for the corresponding Job server. The process steps are requested in the Job queue with exactly these queue names.

- Hardware
  Name of the hardware that the synchronization server is installed on.

- Language
  Language setting for the synchronization server

This data does not, however, have any meaning for the server in its function as synchronization server and therefore, should therefore, not be done until after initial synchronization.

Once the synchronization server has been added to the database, a corresponding entry is made for a Job server that will be responsible for supplying the queue for handling the target system specific processes with Identity Manager Service. This queue needs to be entered into the Identity Manager Service configuration file. Refer to section Configuring a Job Server on page 210 in the Configuration Manual.

Declaring the LDAP Store Server

When actions are executed, the synchronization server communicates with the server stored by LDAP Store. This server is a selected live server with a good network connection to the synchronization server. You must declare this server in the Identity Manager database. Proceed as follows:

- Set up the server in the same way as the synchronization server. Refer to section Declaring the LDAP Synchronization Server on page 403.

- Enable the option <LDAP Store> for the server.

Setting Up an LDAP Domain

Add the synchronization dmain in the Manager in the category <Generic Target Systems>\<Domains> for synchronizing with the Identity Manager database. Enter the data required for the domain on the form <Change master data>

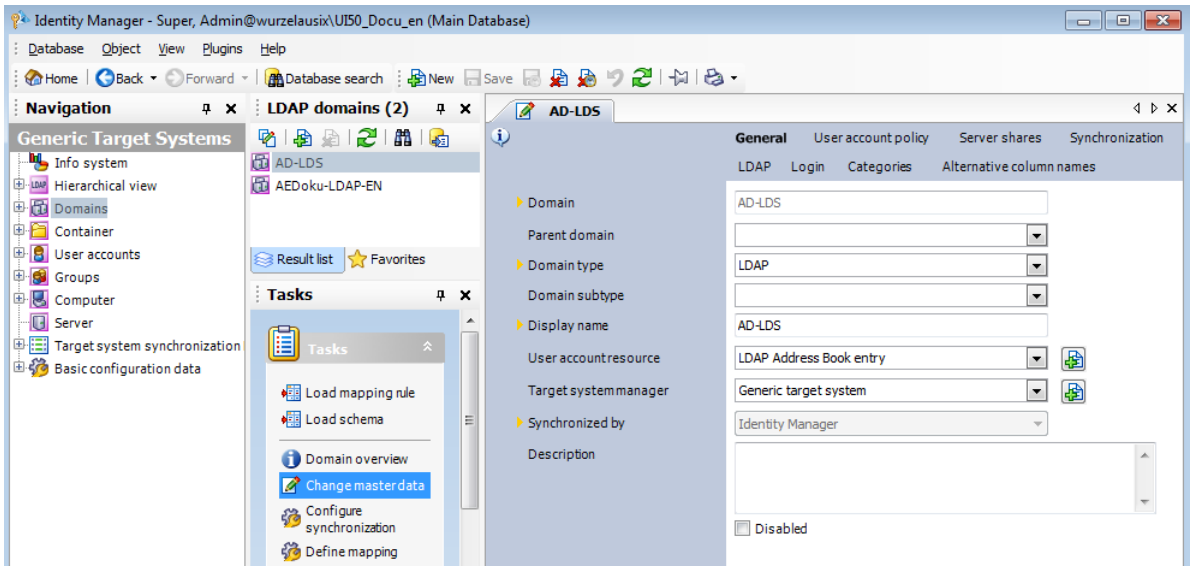
When a domain is set up in the Identity Manager database, a root container with the same name and the object class ”top“ is created automatically. This root container is not distributed in the LDAP environment but is used internally by the Identity Manager database to group and map objects that cannot be assigned to a container in the LDAP directory.

On the <Change master data> form you can enter all the data required for the domain.

General Master Data for an LDAP Domain

Enter the general data for a domain on the <General> tab

Setting Up a Domain



You need to enter at least the following information for the domain:

- Domain name
  Enter the domain name here. The domain name cannot be changed later.

- Parent domain (if exisits)

- Domain type for identifying the domain
  Select the domain type ”LDAP“.

- Synchronized by
  Specify how the data will be synchronized between the domain and the Identity Manager. Choose between ”Identity Manager“, ”FIM“ and ”No synchronization“.

  Identity Manager: data synchronization between the Identity Manager database and the domain is carried out by the synchronization components from the Identity Manager.
  FIM: data synchronization between the Identity Manager database and the domain is carried out by the Microsoft Forefront Identity Manager.
  No synchronization: no changes are automatically transfered from the Identity Manager database to the domain.

  You can only specify the type of synchronization when a new client is added. Once it has been saved, no changes can be made. If you select ”No synchronization“ you can define custom processes to exchange data between the Identity Manager and the domain.

The following input is necessary depending on the selected administration model:

- User account resource
  This input is necessary if user accounts belonging to this domain are to be managed with a user account resource. Read more in the section Login Data for a User Account on page 411.

- Specifies the domain as a master domain if set
- Specifies whether the domain is enabled or temporary disabled.
  This option is evaluated in various processes for the inital filling of a domain.

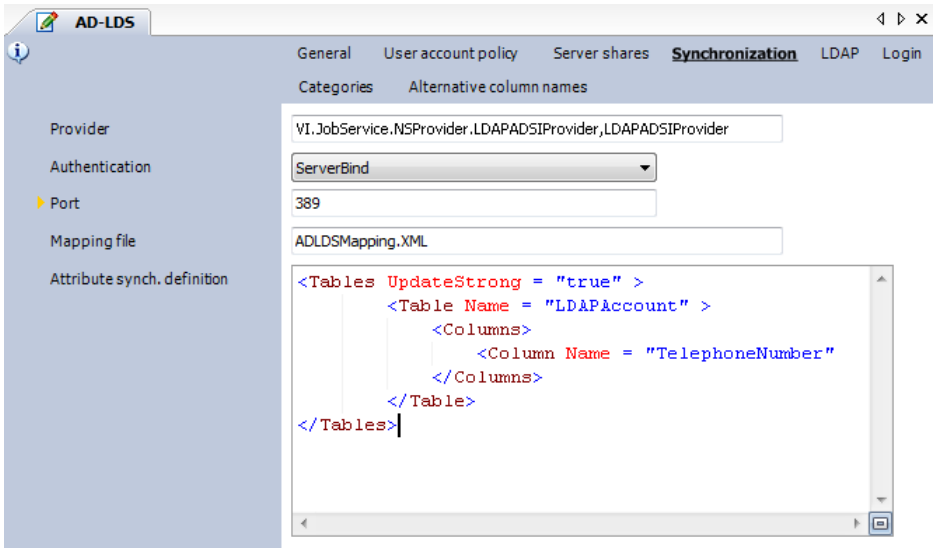
User Account Policy

There is no user account policy in the default installation of the Identity Manager for a domain .

Customizing Synchronization Data

Enter the special options for synchronizing data between the Identity Manager database and the target system environment on the <Synchronization> tab. You can make the changes for each domain because the requirements within a LDAP environment are different from domain to domain.

Customizing Data Synchronization



You can enter the following data for data synchronization:

- Choice of provider
  If a target system has the choice of several providers, one has to be selected here.
  Currently permitted providers are:
  - VI.JobService.NSProvider.LDAPADSIProvider,LDAPADSIProvider
  - VI.JobService.NSProvider.LDAPNovellProvider,LDAPNovellProvider
- Authentication data
  Here you can specify the authentication type for login in addition to user account and password. There are different authentication type to choose from, ”Encryption(SSL)“, ”Secure“ for example.
- Port
  Enter a number for the communications port on the target system server in addition to the user account and the password.
- Mapping file
  The mapping file contains the templates for mapping target system specific objects, such as user accounts, groups or hardware objects, between the Identity Manager database and do-

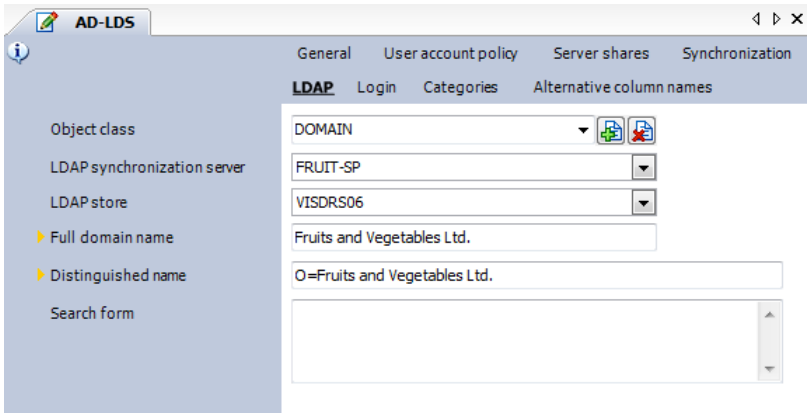
mains. The evaluation is carried out using target system specific process components. An external mapping file only has to be given if the default mapping for the data should not be used. This external mapping file must exist on the synchronization server. If no path is given, the mapping file has to be in the Identity Manager Service install directory on the synchronization server. Refer to the chapter Customizing Mapping rules on page 180 for further infomation.

- Attribute comparison definition
  You can specify the master for data synchronization for individual target specific object properties with the attribute comparison definition. The input is entered in an XML structure. Refer to the section Specifying the Data Master for Object Properties on page 192 for more information.

LDAP Specific Master data

The <LDAP> tab is shown when the when a domain is labeled with the domain type ”LDAP“.

Target System Specific Input for Domains



The following input is required:

- Object class
  The default object class is ”DOMAIN“. You may add other object classes.

- LDAP synchronization server
  Select the server which is going to be the synchronization server. Refer to the section Declaring the LDAP Synchronization Server on page 403.

- LDAP Store
  Enter the server that keeps the LDAP Store. The LDAP synchronization server connects to this server when running target system processes. The LDAP Store server must be declared in the Identity Manager database. Refer to the section Declaring the LDAP Store Server on page 403.

- Full domain name
  Enter the domain name in DNS syntax:

  ```
  This domain name.parent domain name.master domain name
  ```

  Example:

  ```
  Doku.Testlab.dd
  ```

- Defined name
  The defined name is created from the full domain name with a template in default installation. Check the name and pass it on if necessary.

Login Data

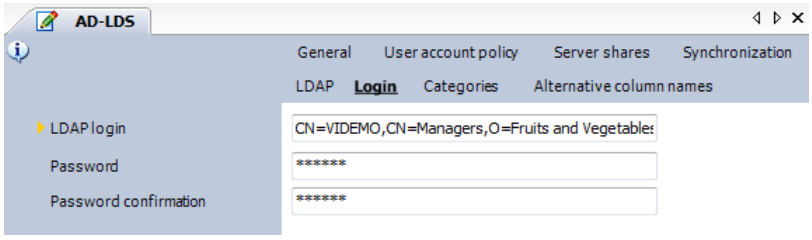
Enter the user account and the password to log into the domain on the <Login> tab. Enter the defined LDAP name as user account.

Example:
The defined LDAP name syntax for the user account ”Administrator“ in the organizational unit (OU) ”System“ in the domain ”Doku.Testlab.dd“ is:

```
CN=Administrator,OU=Users,DC=Doku,DC=Testlab,DC=dd
```

The user account has to be one with administrative permissions in the LDAP environment. This account uses Identity Manager Service to reconcile LDAP object properties.

Domain Login Data



Accelerating Synchronization

Configuration Parameter for Accelerating Synchronization

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\LDAP\UseUSN	When LDAP objects are synchronized, a comparison is carried out using the change date.

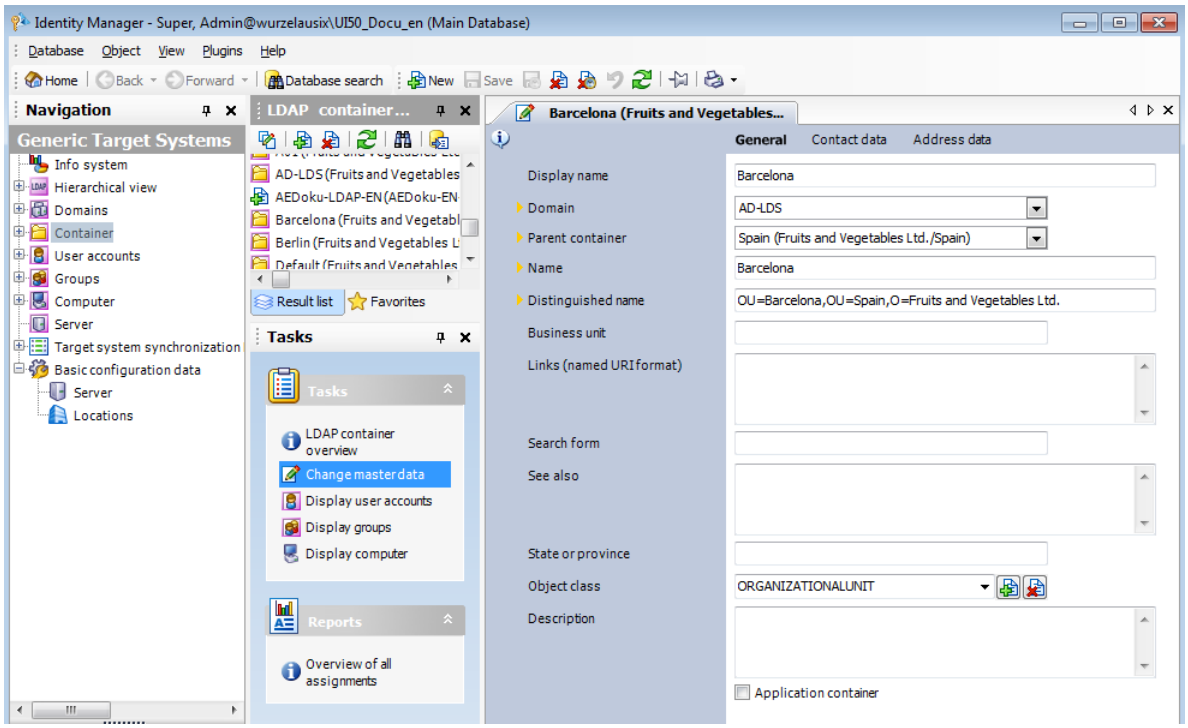
All LDAP objects are loaded individually during synchronization. You can implement a document filter to speed up the synchronization as this procedure can be very time consuming in certain circumstances. Each LDAP object saves the last change date. Each synchronization, using the methods ”ReadAndInsert“ or ”ReadAndUpdate“, saves the last change date in the Identity Manager database. The next time a synchronization is run, only those LDAP objects that have been changed since this date are loaded. This avoids unnecessary updating of objects that have not changed since the last synchronization.

LDAP Container Structures

LDAP containers are represented by a hierarchical tree structure. Containers are often used to display organizational units such as branch offices or departments, to organize LDAP directory objects such as users, groups and computers logically and therefore to ease the burden of object administration. Directory containers are loaded by synchronization with the Identity Manager database. You have the option

to change existing containers in the Manager or to add new ones. The containers are displayed in the category <Generic Target Systems>\<Container>.

Setting Up a Container



Enter a minimum of the following data for a container:

- Container name
- Domain and parent container
  When you set up a domain in the Identity Manager database, a root container with the same name and the object class ”top“ is created automatically. This root container is not distributed in the LDAP environment but is used internally by the Identity Manager database to group and map objects that cannot be assigned to a container in the LDAP directory. When a new container is created, the root container is suggested as parent container. You can, however, specify another parent container in order to implement a hierarchical structure.
- Container’s defined name
  The defined name is made up of the name of the new container and the parent container’s defined name.
- The object class
  New containers are added as organizational units with the object class ”OrganizationalUnit“. You can also add other object classes using the input field.

You can check the assignment of users, groups and computers to the container structure. You can add new users, groups and computers with the appropriate data. Use the task to preset container data in the respective LDAP objects.

LDAP User Accounts

Configuration Parameter for Setting up User Accounts

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\LDAP\PersonAuto-Default	Depending on this parameter the decision is made as to whether automatic assignment of employee should come into effect when a user account is added (not active for synchronization).
TargetSystem\LDAP\PersonAuto-FullSync	Depending on this parameter the decision is made as to whether automatic assignment of employee should come into effect when a user account is added during synchronization.

You can use the Identity Manager to manage user accounts in an LDAP environment. A user account can login in to a domain and receive group memberships and access rights to network resources.

The Identity Manager uses several method to create user accounts and assign them to employees.

- Employees and user accounts can be entered manually and assigned to each other.
- Employees can automatically obtain their user accounts using user account resources. If an employee does not have a user account in a domain, a new user account is created. This is done by assigning user account resources to an employee using the integrated inheritance mechanism followed by process handling. This method is described in more detail in the section Login Data for a User Account on page 411.
- When a user account is added, an existing employee is automatically added or a new one is created if necessary. In the process, the employee master data is created based for existing user accounts. This mechanism can follow the creation of a new user account by manual addition or by synchronization. This method, however, is not the Identity Manager default method. This method is explained in section Login Data for a User Account on page 411.

The basic mechanisms are dealt with in the chapter Employees and User Accounts on page 25.

Entering LDAP User Account Master Data

A user account can be connected to an employee in the Identity Manager. User accounts can also be managed separately from employees, for example, when dealing with administration user accounts.

user accounts are displayed in the Manager in the category <Generic Target Systems>\<User accounts>. On the <Change master data> form you can manually enter the required data for a user account and edit it if necessary. Ensure that you fill in all compulsory fields.

We recommend that you use user account resources to set up user accounts for company employees. If you use a user account resource to set up a user account, some of the master data that is described in the following, i.e. container, is created using templates. Certain employee master data is inherited using employee user account templates. In this case, the scope of the data is based on the default manage level for the user accounts resource. The templates supplied should be customized as required.

General Master Data for a User Account

Enter the master data for a user account on the tab <General>. You may assign an employee to a user account from the <Employee> pop-up list. If the user account was created using a user account resource, an employee will already be entered. If you use automatic employee assignment, a associated employee is created and entered into the user account when the user account is saved. If you do not

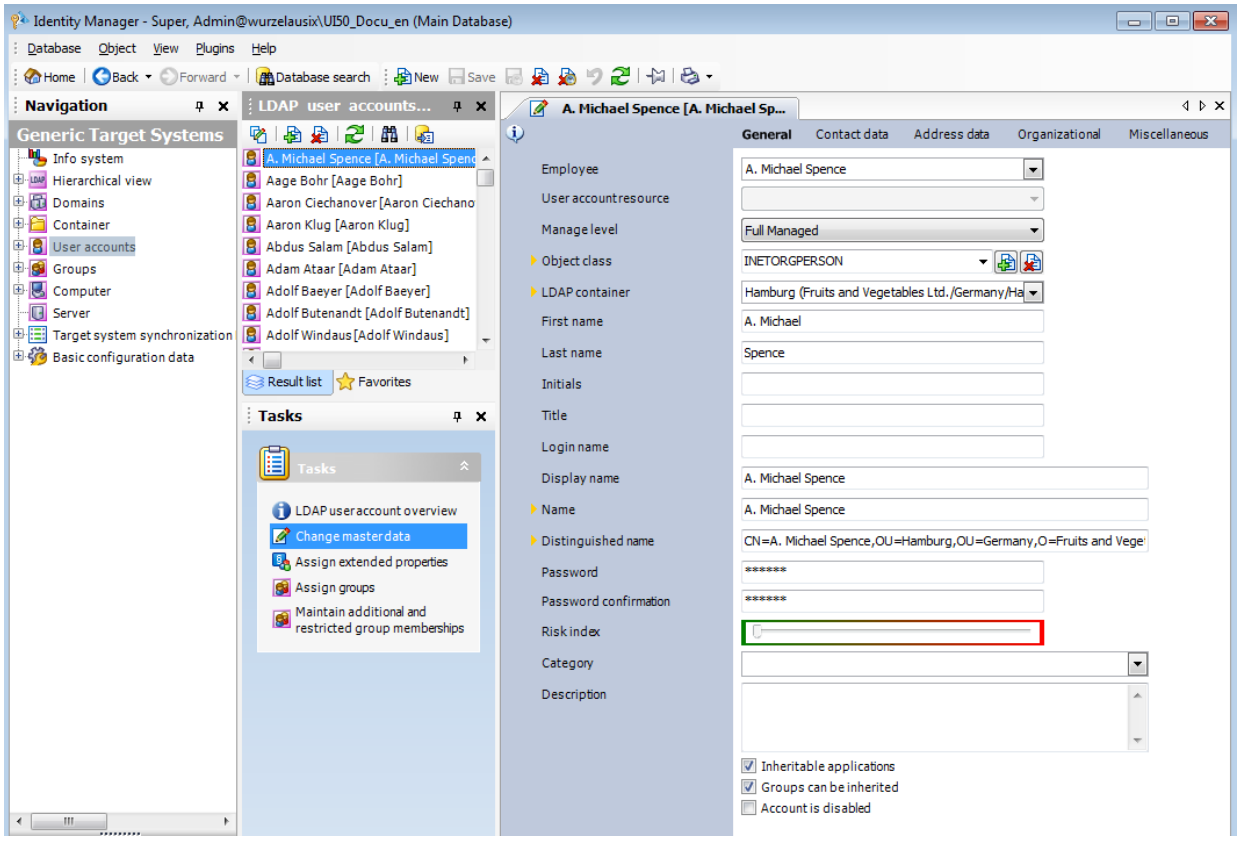
use any of these methods but manually create the user account, you can also assign an employee manually to the user account.

When user account resources are assigned to an employee or a resource to a company structure, an associated user account is created with the integrated inheritance mechanism and the process handling that follows. If the process handling fails because, for example, not all the neccesary IT operating data could be found, you can also create the user account manually and, at the same time, select the user account resource to use. Only the user account resources that are already assigned to the employee are shown in the pop-up menu <User account resource>.

The user account manage level is decided by the range of the employee's properties that are passed on to the user account. The Identity Manager's default installation is configured for the manage levels "Unmanaged" and "Full managed". User accounts with the manage level "Unmanaged" are merely linked to an employee but do not inherit other properties. User accounts with the manage level "Full managed" inherit defined employee properties. You can define other manage levels depending on the company's requirements.

When a user account is created using a user account resource, the default manage level of the user account resource is used and is transfered to the user account. Normally, the manage level "Full managed" is used as default. If you create the user account manually or with automatic employee assignment, the manage level is "Unmanaged". You can change the levels after the user account has been saved, provided that the domain has a user account resource.

General Master Data for a User Account



Enter the general data for the user account such as name, surname and initials if necessary. This data is used to create the display name and the user account name. Select the container for creating the user. The container is determined by the valid IT operating data for the assigned employee depending on the user account manage level. When the container is selected, the defined name for the user is created using a formatting rule.

By default, user accounts are added with the object class ”InetOrgPerson“. However, you can add object classes through the input field that are used by other LDAP and X.500 directory services to map user accounts.

You can assign an employee applications and application packets. If the employee has a user account, then this account becomes a member in the application’s group. The option <Inheritable applications> needs to be set as prerequisite for adding the user account in the application group. Another prerequisite is the existence of the application group in the user account domain. The DBScheduler calculates the application assignment depending on this.

The option <Inherit groups> effects inheritance of user account group memberships. If an employee with a user account is added, for example, to an Identity Manager business role and if groups are assigned to this business role, then the user account indirectly inherits assignment to the group. Inheritance of group memberships is described in section How LDAP User Accounts Inherit LDAP Groups on page 299 in the Configuration Manual.

Login Data for a User Account

Configuration Parameters for password data

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\LDAP\Accounts\InitialPassword	This configuration parameter contains the initial password for newly created user accounts.
TargetSystem\LDAP\Accounts\InitialRandomPassword	A random generated password is generated when a new user account is added. It must contain at least the character classes that are set in the child configuration parameters.

Enter the user account login data on the <General> tab. The user account needs a login name to login to the LDAP directory. The login name is formed from the login name in the employees central user account depending on the user account manage level. Provide a password for the user account.

You can set an initial password for newly added user accounts with the configuration parameter ”TargetSystem\LDAP\Accounts\InitialPassword“. Use the parameter ”TargetSystem\LDAP\Accounts\InitialRandomPassword“ to specify whether a randomly generated password should be issued to a new user account. The child parameters specify the character sets that the password needs to contain and the email address that the password should be sent to. Depending on the configuration parameter ”QER\Person\UseCentralPassword“, the employee’s main password can be mapped from the user account password.

Additional Master Data for a User Account

Enter the contact data for a user account, e,g, telephone number or extra email addresses, on the <Contact data> tab. Enter address data on the <Address data> tab. On the <Organizational> tab, enter the personnel number, detailed job description and an LDAP account manager along with data for user’s organizational affiliations such as, department, location or country ID. Enter the default PC, user ID and description of the user account on the <Miscellaneous> tab.

Additional Tasks for Managing User Accounts

After you have entered the user account master data, you can apply different tasks to it. You can see the most important information about the user account on the overview form. The task view contains different forms with which you can run the following tasks.

Assign groups directly to User Accounts

All groups are shown on the overview form. groups can be assigned directly or indirectly. Indirect assignment is carried out by allocating the employee and the groups to roles. If the employee has a user account, the Lotus Notes groups in the role are inherited by the user acount. To react quickly to special requests, you can assign groups directly to the user account. To do this you use the for <Assign groups>. See section Assigning Company Resources through Roles on page 78 for more information on group management.

Managing User Account through User Account Resources

You can automatically create user accounts for company employees with the help of user account resources. You can set up user account resources for any domain in an LDAP environment. The basic mechanisms are explained in the section Creating User Accounts with User Account Resources on page 37.

Should an employee get a user account through user account resources, he or she must have a central user account and receive the IT operating data over a primary department, location or cost center assignment. Read more in section Handling Employees and User Accounts on page 30.

In the default installation, there is a test to see if a user account already exists in the user account resource domain. If there is no user account, a new user account is created with the user account resource default manage level. If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

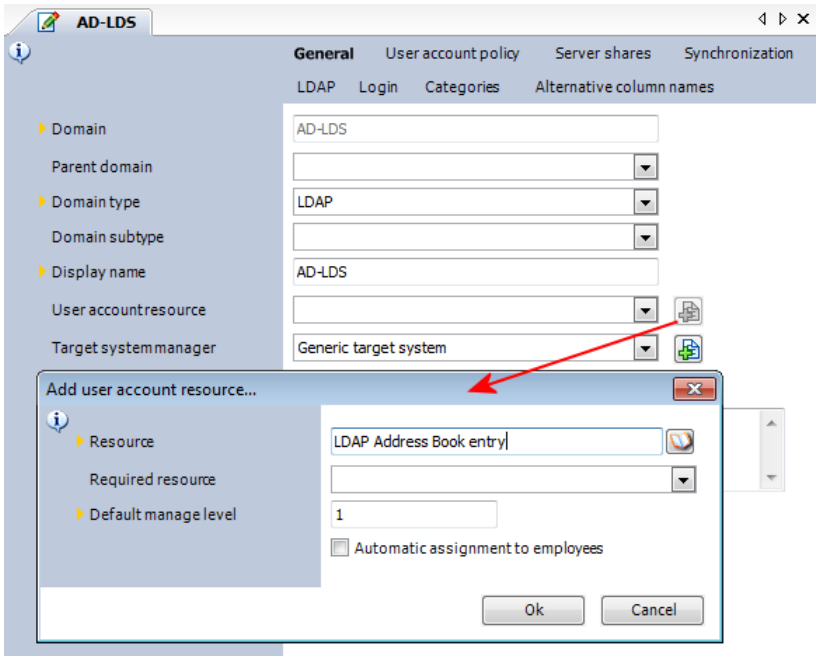
Creating a User Account Resource for a Domain

Configuration Paramater for User Account Resources

CONFIGURATION PARAMETER	MEANING
TargetSystem\LDAP\UniqueDefaultManageLevel	When the parameter is set, a different default manage level is expected for each user account resource in the target system (default). If the parameter is not set, each user account resource in the target system may have the same default manage level.

You can set up a user account resource for a domain in the category <Generic Target Systems>\<Domains>. Enter the data for the new user account resource on the domain's master data form by clicking the button next to the corresponding field.

Setting up a User Account Resource for a Domain



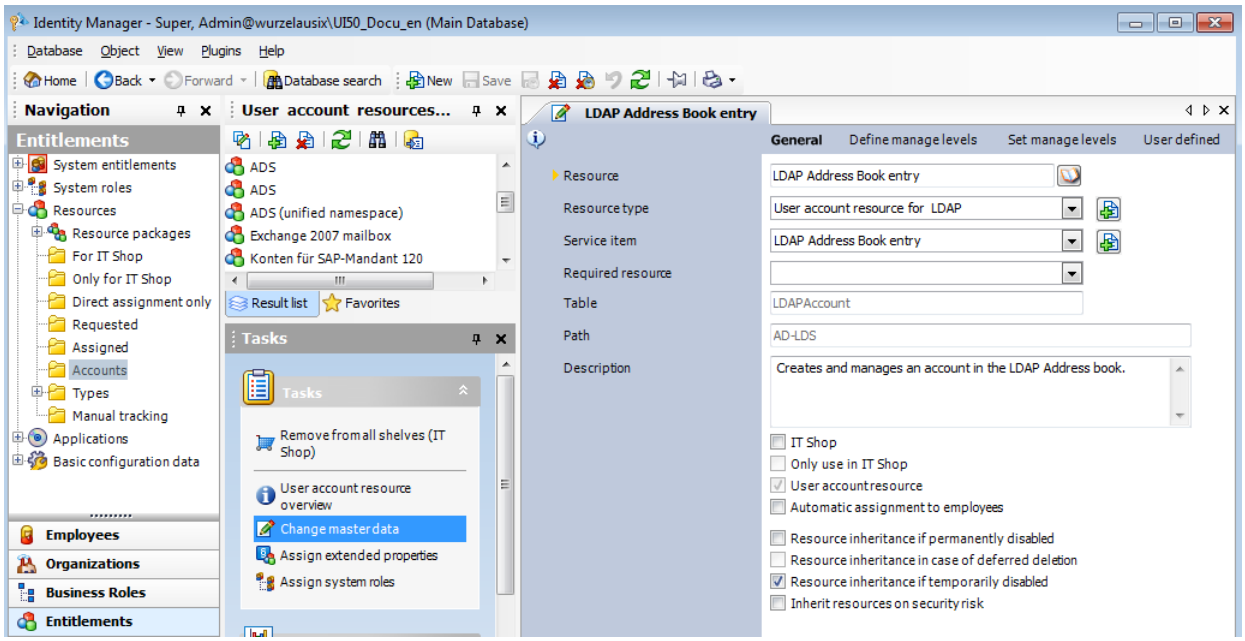
Enter the following data for the user account resources:

- Resource identifier
- Default manage level
  The Identity Manager's default installation is configured for the manage levels "Unmanaged" and "Full managed". User accounts with the manage level "Unmanaged" are merely linked to an employee but do not inherit other properties. User accounts with the manage level "Full managed" inherit defined employee properties. You can define other manage levels depending on the company's requirements. Refer to section Specifying Manage Levels for Handling User Accounts on page 415 for more information.
- Assumed resource
  This field defines a dependency between user account resources. Leave this field empty for a domain.

- Automatic assignment to employees
  Label the user account resource with this option when it should be automatically assigned to all internal employees. The user account is assigned to every employee that is not marked as external on saving. The moment a new employee is added, they also are assigned this user account.The assignment is computed by the DBScheduler.

A new user account resource is created when the data is saved. You can subsequently edit the other data for this user account resource in the category <Resources & Groups>\<Resources> in the filter <Accounts>.

Reworking the User Account Resource



Additional data for user account resources is:

- A resource type.
  Resources should obtain a resource type. This resource type defines future post-processing steps for resource requests or resource assignments.

- The base table in which the user is displayed.
  This input is preset with the value ”LDAPAccount“ when the user account resource is assigned to a domain and cannot be changed.

- The domain path used by the user account resources
  This input is preset with the NetBIOS name of the domain when the user account resource is assigned to a domain and cannot be changed.

- Service item
  Assign a <service item> to the resource or add a new one. This way the resource can be booked internally.

- Data for use in IT Shop
  Mark a user account resource with the option <IT Shop> if it is going to be requestable in the IT Shop (see Chapter Setting Up an IT Shop Solution on page 15). These user account resources can be requested by the employees over a web front-end and distributed with a defined approval policy. The user account resource can still, however, be assigned directly to an employee and non-IT Shop roles. In order to avoid direct assignment, activate the option <Only use in IT Shop>. In this case user account resources can only be requested through the IT Shop.

- Data when a currently disabled employee inherits the resource
  You define the inheritance behavior of the user account resource yourself. The inheritance options of the previous resources are overwritten. This resource inheritance behavior may be desired in order to, for example, ensure that all required permissions are immediately reinstated for an employee that is reactivated at a later date. The user account resource options <Resource inheritance if permanently disabled>, <Resource inheritance if temporarily disabled> and <Inherit on security risk> are available to map the inheritance behavior. If the user account resource is not passed on when an employee is disabled, the connected employee user account, that was created by assigning this resource, is deleted.

Specifying Manage Levels for Handling User Accounts

You can specify the manage level for a user account resource for handling user accounts. These manage levels are the basis of the manage levels permitted for user accounts. The user account manage level determines the scope of the properties that a user account inherits from an employee.

Therefore, an employee can, for example, have several user accounts in a domain:

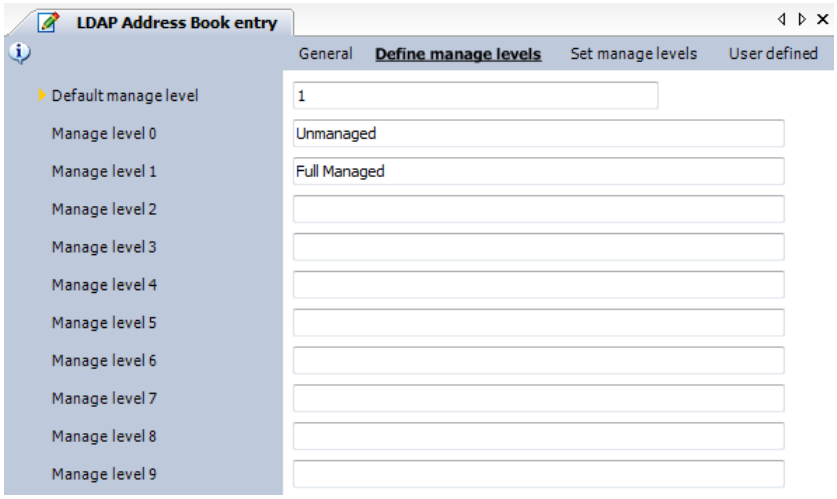
- Default user account that inherits all properties through the employee
- Administrator user account that although linked to the employee, should not inherit any properties.
- Service account, which obtains, for example, the home and profile directories from the employee but does not inherit other properties

The Identity Manager supplies a configuration for the 0 manage level with manage level ”Unmanaged“ and the manage level 1 with manage level ”Full managed“. These manage levels are taken into account in the templates. User accounts with an manage level of ”Unmanaged“ inherit defined properties from the assigned employee. These manage level are taken into account in the templates. You can define more manage levels depending on you requirements. Then you need to extend your templates to include the methods for the additional manage levels.

When user account resource is assigned to an employee, the default manage level is used to create the user account resource. If more domains should be managed using user account resources, you have create a separate user account resource per domain. In the default installation each target system user account resource is expected to have a different default manage level. However, the Identity Manager allows several user account resources with the same default manage level to be used. The desired behavior can be controlled with the configuration parameter ”TargetSystem\LDAP\UniqueDefaultManage-

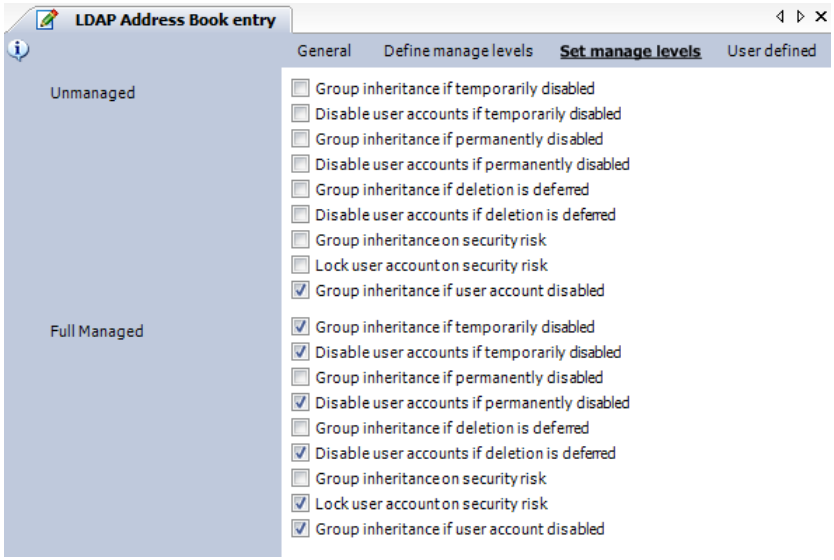
Level". There is an example in section Creating User Accounts with User Account Resources on page 37 which explains this in more detail.

Manage Levels for Domain User Account Resources



For each manage level, you need to specify the effects of temporary or permanent disabling and deletion of an employee on his or hers user accounts and group memberships.

Editing User Account Resource Manage Levels


LDAP Address Book entry
General
Define manage levels
Set manage levels
User defined
Unmanaged
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled
Full Managed
Group inheritance if temporarily disabled
Disable user accounts if temporarily disabled
Group inheritance if permanently disabled
Disable user accounts if permanently disabled
Group inheritance if deletion is deferred
Disable user accounts if deletion is deferred
Group inheritance on security risk
Lock user account on security risk
Group inheritance if user account disabled

The employee's user account can be locked when he or she is disabled or deleted so that permissions are immediately withdrawn. If an employee is re-enabled at a later date, the user accounts can also be reactivated. This behavior is controlled by the properties:

- Disable user accounts if permanently disabled
- Disable user accounts if temporarily disabled
- Disable user accounts if deletion is delayed
- Disable user accounts if security is at risk

Group membership inheritance can be define for a user account resource for an area of a target system. Inheritance may be discontinued if the employee's user account is locked and therefore may not become a member in a global group. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted! This behavior is controlled by the properties:

- Group inheritance if permanently disabled
- Group inheritance if temporarily disabled
- Group inheritance if deletion is delayed
- Group inheritance if security is at risk

You can find further information in the section Handling Disabling and Deletion of Employees and User Accounts on page 44.

Deleting User Accounts

Effective Configuration Parameters when Deleting User Accounts

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\LDAP\Accounts\Initial-Password	Initial user account password
QER\Person\User\DeleteDelay	Delay on deletion

When a user account is deleted in the Identity Manager, the user is initially disacbled and is given a random password. This removes any access to the LDAP directory. The user account is finally deleted from the target system and the Identity Manager database depending on the setting of the configuration parameters "QER\Person\User\DeleteDelay". During this time it is possible, using the context menu entry <Reset delete>, to reset the status to "changed". In the default installation the user account password is reset to the initial password stored in the configuration parameter "TargetSystem\LDAP\Accounts\InitialPassword".

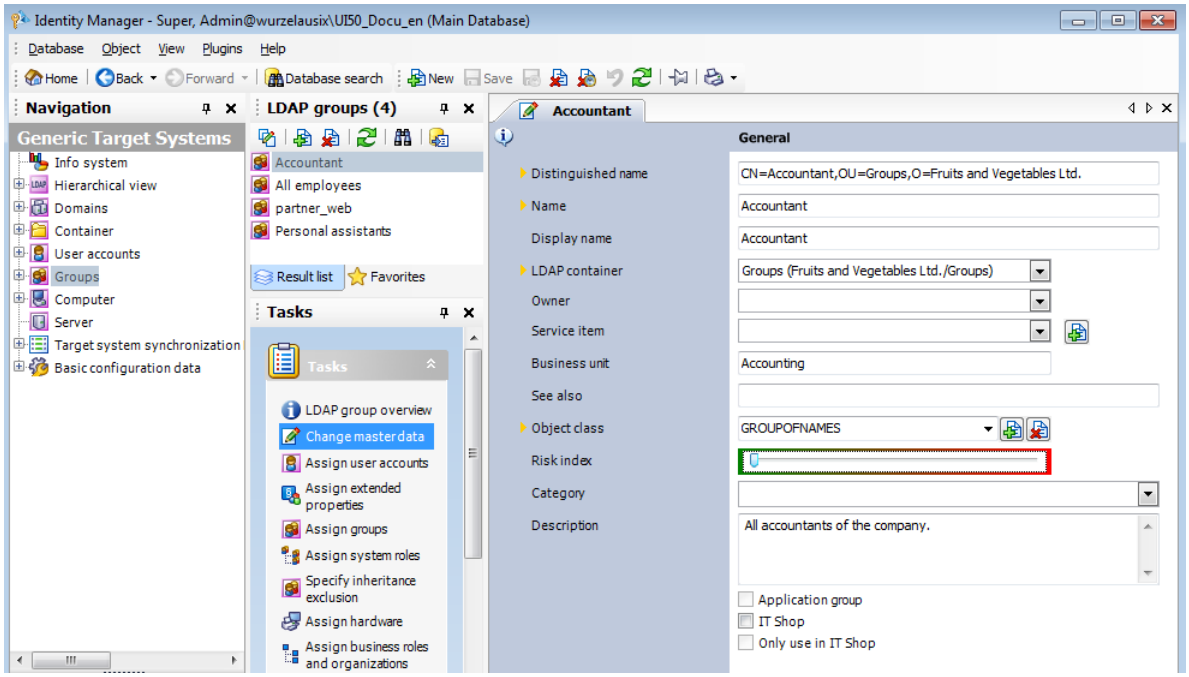
LDAP Groups

Effective Configuration Parameter

CONFIGURATION PARAMETER	EFFECT WHEN SET
TargetSystem\LDAP\MemberProperties	groups are represented by different object classes in the LDAP schema. Each object class is expected to have a different attribute to represent the group memberships. The assignment of object classes to properties is achieved using the configuration parameters: - TargetSystem\LDAP\MemberProperties\GroupOfNames - TargetSystem\LDAP\MemberProperties\GroupOfUniqueNames - TargetSystem\LDAP\MemberProperties\OrganizationalRole These are used in generating processes by the assignment of group memberships.

You can collect user accounts, contacts, computers and groups into groups that can be used to regulate access to resources. You can use the Manager to set up new groups or to edit existing groups. groups are displayed in the category <Generic Target Systems>\<Groups>.

Creating an LDAP Group



Enter the following data for a group:

- Group name
- LDAP Container
  Select the container to add the group to. The defined name is created using a template from the group name and the container name.
- Defined group name
  The defined name is created from the group name and the container name.

- Object class
  groups are represented by various object classes in the LDAP schema.A different property is expected for each object class for mapping group memberships in LDAP. Use the configuration parameter ”ameSpace\LDAP\MemberProperties“ and its child parameters, to specify the LDAP object class property that the group memberships will mapped to.
  New groups are added with the object class ”groupOfNames“. Use the button next to the input field to add other object classes or to delete unused ones.

- Application group flag
  This option is automatically set when an application group is created and therefore, should not be manually edited. Particularities of application group administration in the LDAP environment can be found in the Configuration Manual in the section Managing Application Groups in Active Directory on page 286.

- IT Shop and service item
  Label the SAP groups, SAP roles and SAP profiles that can be requested through the IT Shop with the option <IT Shop>. These groups can be requested by their staff members through the web front-end and distributed using defined approval policies. The groups can, however, still be assigned directly to employees, user accounts and non-IT Shop roles. To prevent direct assignment, enable the option <Only use in IT Shop>. In this case, groups can only be requested through the IT Shop. To use a group within the IT Shop, assign an service item to it or add a new service item. This allows the group to be booked internally.

Additional Tasks for Managing Groups

After you have entered the group master data, you can apply different tasks to the groups. You can see the most important information about a group on the overview form. The task view contains different forms with which you can run the following tasks.

Add Groups to Company Structures

It is possible for user accounts to inherit these groups if groups are assigned to individual company structures. Groups are added to departments, cost centers, locations or business roles. If an employee is added to one of these company structures and this employee has user accounts where the <Groups can be inherited> option set, then these accounts become members of the group. You can find further information in the section Assigning Company Resources through Roles on page 78.

Inheritance processes are calculated by the DBScheduler. Group inheritance is described in the section How LDAP User Accounts Inherit LDAP Groups on page 299 described in the Configuration Manual. A mechanism to monitor membership has been implemented in LDAP becuase the number of members in a group is limited. See section Managing Application Groups in LDAP on page 301 in the Configuration Manual.

Add Groups to IT Shop

When groups are assigned to an IT Shop shelf the groups can be requested from the shop’s customers. To ensure the group is requestable there are further prerequisites need to be guaranteed. There is more information about this in the section Requestable Products on page 33. To remove a group from the IT Shop, use the task <Remove from all shelves (IT Shop)>.

Add User Accounts and Groups directly to Groups

Use the forms <Assign user accounts> and <Assign groups> to directly assign groups directly to user accounts and other groups.

Specify Dependencies between Groups

Use the form <Specify inheritance exclusion> to define dependencies between groups as long as the configuration parameter ”QER\Inherite\GroupExclusion‟ is enable. By defining dependencies between the groups, the number of resulting memberships of user accounts is reduced in the groups. Read more in section Inheritance Exclusion on page 80.

Assign Extended Properties to Groups

Extended properties are meta objects for which there is no direct mapping, such as accounting codes, controlling areas or cost center areas, in the Identity Manager data model. These extended properties are used to check rule conformity. For more information see section Setting Up Extended Properties on page 424.

Deleting Groups

A group can be deleted over the result list context menu or menu items. After confirming the deletion query, the group is marked to be deleted and is finally removed from the database by Identity Manager Service.

13

Rule Compliance in the Identity Manager

- Introduction
- Setting up a Rule Base
- Rule Checking
- SAP Functions

Introduction

In recent years, many countries and economic unions have adopted general or industry specific laws and regulations that have an a growing influence on companies' IT environments.

The law that is currently discussed the most is the Sarbanes-Oxley Act (SOX) from the USA, which improves company reporting. The German law for controlling and transparancy in company environments (KonTraG) and the 8th EU directive (SOX for europe) have similar aims. Industry specific rules such as banking laws or Food&Drug Association (FDA) regulations represent other such challenges.

The Identity Manager can be used to define rules that maintain and monitor regulatory requirements and automatically deal with rule violations. On the one hand, rules are used for locating rule violations and on the other hand, to prevent them.

Simple rule examples are:

- An employee may not obtain two entitlements A and B at the same time.
- Only employees with a particular department can have a particular permission.
- Every user account has to have a manager assigned to it.

You can use the audit function from the Identity Manager to:

- Define rules for any employee assignments
- Evaluate the risk of possible rule violations
- Specify mitigating controls
- Initiate regular or spontaneous rule checks
- Detailed testing of edit permissions for employees within an SAP client (using SAP functions)
- Evaluate rule violations with differingcriteria
- Create reports about rules and rule violations

Based on this information, you can made corrections to data in the Identity Manager and transfer them to the connected target systems. The integrated report function in the Identity Manager can be used to provide the information for the appropiate tests.

Setting up a Rule Base

General Configuration Parameters for Rule Compliance

CONFIGURATION PARAMETER	MEANING
QER\ComplianceCheck	Preprocessor relevant configuration parameter for controlling the database model components for checking the rule base. Changes to the parameter require recompiling the database. If this parameter is enabled, you can use the model components.
QER\ComplianceCheck\Simple-Mode	Preprocessor relevant configuration parameter for controlling the definition of rule conditions for compliance rules. Changes to the parameter require recompiling the database. If this parameter is enabled, you can use the model components.

You can define rules for maintaining and monitoring regulatory requirements in a rule base. A rule in the Identity Manager not only contains a technical description but also properties such as rule violation level, owner, manager or audit information. The rules can be also classified into categories (”compliance framework“) and rule groups.

Define a set of rules in Identity Manager in the category <Identity Audit>. To do this, login with a role based authentication module from the application role <Identity Audit>\<Administrators>. You can also defin a rule set in the Manager.

Base Data for Setting up Rules

Enter the rule’s base data in the category <Identity Audit> in <Basic configuration data>. The following base data are relevant for creating rules in the Manager:

- Rule groups
  Use rule groups to group rules by functionality, for example, to group account policies or separate functions (”Segregation of duties“).

- Compliance frameworks
  Compliance frameworks are used to classify rules according to regulations such as internal requirements, auditing requirements or those arising from SOX.

- Extended properties
  You can use extended properties to access properties in rule conditions that are not mapped in the Identity Manager data model. It may be necessary, depending on the range of rule base, to maintain a large number of extended properties. Therefore, you can group properties into property groups. Read more in the section Setting Up Extended Properties on page 424.

- Process schedules
  Scheduled tasks are created for regularly testing the rules. How to create and configure scheduled tasks is described in more detail in section Setting Up a Scheduled Task to Calculate Dynamic Roles on page 103.

- Mitigating controls
  Risk of rule violations can be reduced with the appropriate controls. For example, regular manual testing of disallowed entitlements can be used to reduce the risk connected with these rule violations. Read section Setting up Mitigating Controls on page 428 about setting up mitigating controls.

- Functional area
  Set up functional areas for the analysis of rule checks of different roles in the context of identity audit. Assign these functional areas to departments, cost centers, locations or business roles. Specify how many rule violations are permitted in a functional area or a role for the compliance rule check. Assign these functional areas to the compliance rules required for the analysis. Section Functional Areas on page 86 describes how to set up functional areas.

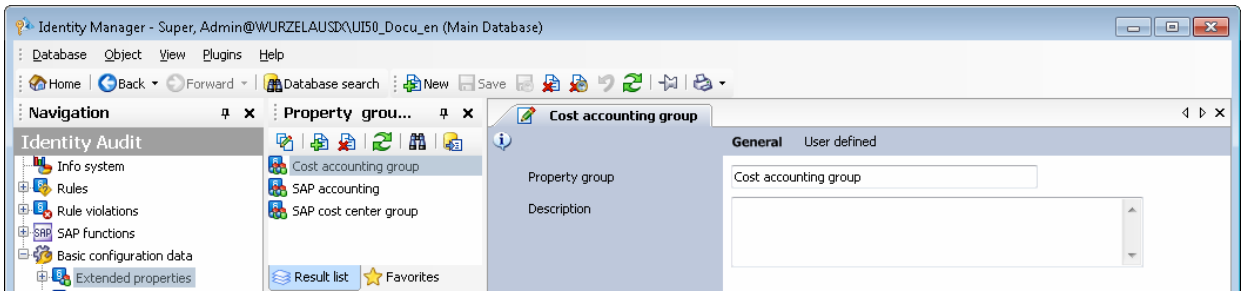
- Attestor
  Employees that can be used to attest attestation procedures can be assigned to compliance rules. To do this, assign an application role <Attestor> to a compliance rule on the master data form. Assign employees to this application role that are authorized to attest compliance rules.
  Edit attestors in the Manager in the category <Identity Audit>\<Basic configuration data>\<Attestor> or in the Identity Manager in the categorie <Identity Manager Administration>\<Identity Audit>\<Attestor>. For detailed information about application roles refer to section The Identity Manager Roles Model on page 61. Refer to section General Master Data for a Rule on page 431 about how to assign attestors to compliance rules.

Setting Up Extended Properties

You can access all the columns and tables of the Identity Manager's data model in a rule condition. However, to establish rules for associated objects, such as accounting codes, controlling areas or cost center areas, you need to set up extended properties.

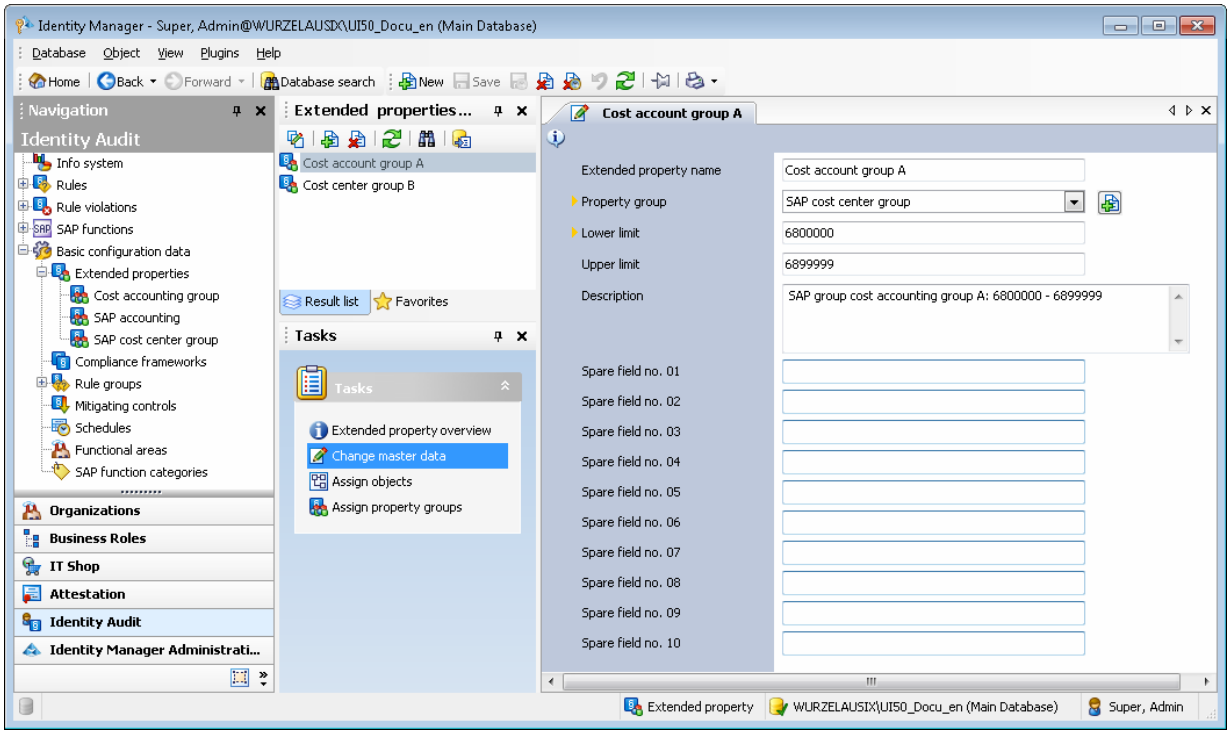
The extended properties and the property groups are displayed in the category <Identity Audit>\<Basic configuration data>\<Extended Properties>. First you set up the property group, under which the extended properties will be grouped. Enter a name and description for the property group.

Setting Up an Property Group



Set up the extended properties in the property group.

Setting up Extended Properties



Enter the following data:

- Extended property name
  Use this name to access the extended property in the rule condition.

- Property group
  Property groups are used to stucture the extended property. You can assign a primary property group to a property on the master data form. If an extended property needs to be assigned to several property groups, then you can use the assignment form <Assign property groups> to assign additional property groups.

- Scoped Boundaries
  You can subdivide extended properties into smaller scopes. You may use the names for the upper and lower scope boundaries in the rule condition. Read the section Specifying Scoped Boundaries on page 426 for more information about specifying division scope and their usage in rule conditions.

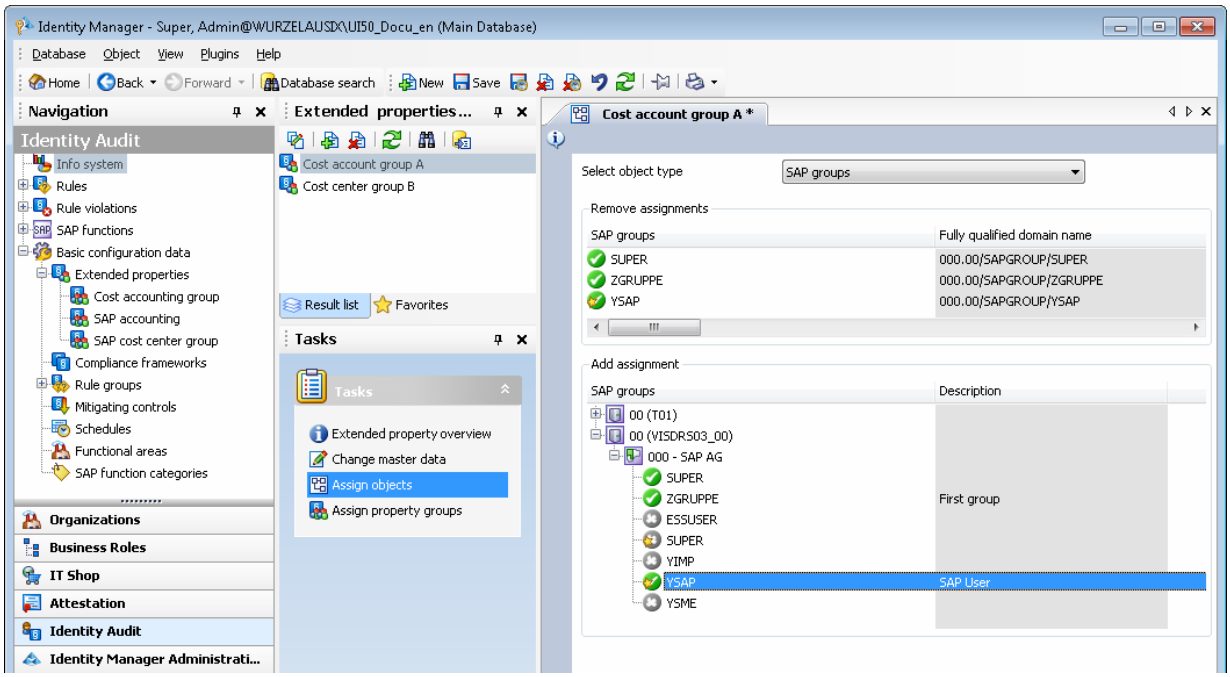
- Description of the extended property

- Spare fields no. 01.....spare field no. 10
  Create any additional company specific information about the extended property.

In order to use extended properties in a rule condition, you have to assign them to the Identity Manager data model objects in the next step. Run the task <Assign objects>. First of all you need to select the object type. The objects are displayed on the form that correspond to the selected type. These can

be assigned to the extended property. Any number of objects from different object types can be assigned to the extended property at this point.

Assigning Objects to an Extended Property



Specifying Scoped Boundaries

You can subdivide extended properties by specifying scoped boundaries. You are not obliged to enter scoped boundaries. If you do enter a lower boundary you are not required to enter an upper one. However, if you specify an upper boundary, you have to enter a lower one.

Take note of the following when defining scoped boundaries:

- Basically, any string is permitted as a lower or upper scoped boundary.
- You can use '*' as a wildcard for any number of characters (even null).
- Wildcards can only be added to the end of a string, e.g. AB*. Strings such as *AB or A*B are not allowed.
- If you enter a lower boundary without a wildcard, you cannot use a wildcard in the upper boundary.

The following restrictions apply for the length of the string:

- If you enter a lower and upper boundary without a wildcard, the strings have to be the same length, e.g. lower boundary 123/upper boundary 456. A lower boundary of 123 and an upper of 45, for example, is not permitted or a lower boundary 123/upper boundary 4567 is also not allowed.
- If you use a wildcard in the lower boundary but none in the upper boundary, then the length of the upper boundary string needs to be the same as or bigger than the string in the lower boundary.

- If you use a wildcard in the lower and upper boundary, they have to be the same length, e.g. lower boundary 123*/upper boundary 456*. A lower boundary of 123* and an upper of 45*, for example, is not permitted or a lower boundary 123*/upper boundary 4567* is also not allowed.

Risk Evaluation

Configuration Parameter for Risk Evaluation

CONFIGURATION PARAMETER	MEANING WHEN SET
QER\ComplianceCheck\Calculate-RiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to this parameter require compiling the database. If the parameter is set, value for the risk index can be entered and calculated.

You can use the Identity Manager to evaluate the risk of rule violations. To do this, enter a risk index for the rule. The risk index specifies the risk involved for the company if the rule is violated. The risk index is given as a number in the range 0..1. By doing this you specify whether a rule violation is not considered a risk for the company (risk index = 0) or whether every rule violation poses a problem (risk index = 1).

The risk index can be entered for the following objects in the Identity Manager.

Risk Index for Identity Manager Objects

OBJECT	EXAMPLE
Compliance rules	Risk for the company if the rule is violated.
Active Directory groups SAP groups, roles, profiles structural profiles Structural Profiles LDAP groups Lotus Notes groups SharePoint groups SharePoint roles System entitlements	Risk for the company if the object is assigned to a user account.
Active Directory user accounts SAP user accounts LDAP user accounts Lotus Notes user accounts SharePoint user accounts User accounts	Risk for the company if the object is assigned to an employee. The risk index is calculated from the risk index values of all assigned groups (roles, profiles) and also system entitlements.
Departments, locations, cost centers, business roles	Risk for the company if an employee that is a member of this role, violates a compliance rule.

You can customize the significance of the values in the risk index. To continue using these values you define a process. The Identity Manager only supplies predefined processes for calculating the risk index for user accounts. Read the section Handling Processes in Identity Manager on page 37 in the Process Orchestration Manual for more information about how to define processes in the Identity Manager. You can create several reports with the Report Editor to evaluate objects, assignments and rule violations depending on the risk index. For more information, read the section Reports in the Identity Manager on page 359 in the Configuration Manual.

When a rule condition is created, the group risk index can already be included as an object property. By using rules of this type you can prevent groups that exceed a specified risk index from being requested in the IT Shop. Read section Creating Rule Conditions on page 439 about how to create rule conditions. Find the details about testing compliance rules for IT Shop requests in section Testing Requests for Rule Compliance on page 68 in the IT Shop Manual.

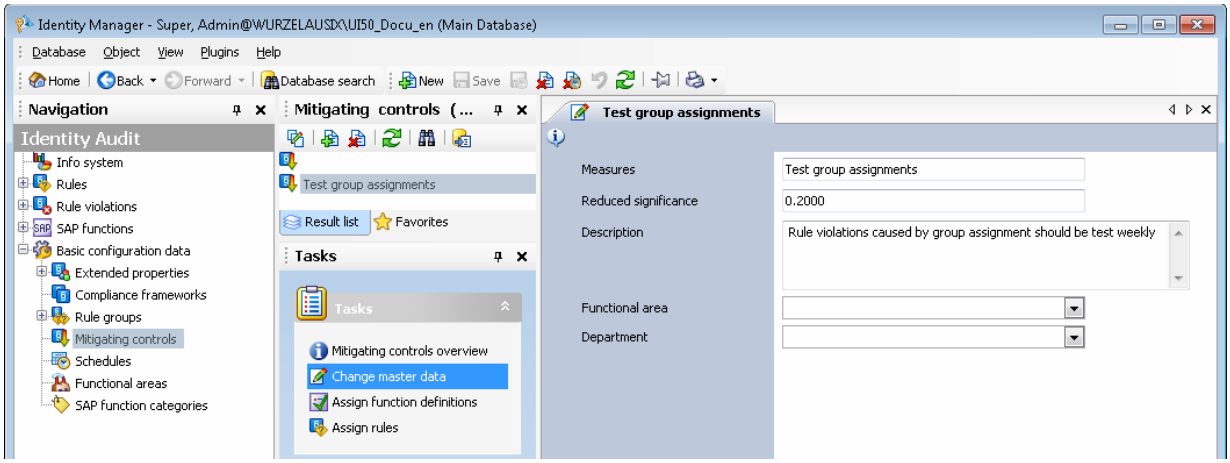
Setting up Mitigating Controls

Mitigating controls can be stored with rules. This is supposed to reduce the risk of rule violations. This means that you specify how rule violation should be dealt with. Mitigating controls do not depend on the Identity Manager functions. For example, regular manual testing of disallowed entitlements can be used to reduce the risk connected with these rule violations.

Migitating controls can also be stored with SAP functions. These reduce the risk of the effects that arise for the company when an SAP user matches an SAP function. At the same time, you specify how to deal with SAP users that match with SAP functions. For example, changes to an SAP role user assignment in the SAP system can represent a suitable mitigating control for an SAP function. Read the section SAP Functions on page 456 for more information about SAP functions.

Mitigating controls are displayed in the category <Identity Audit>\<Basic configuration data>\<Mitigating controls>.

Setting up Mitigating Controls



Enter the following master data for mitigating controls:

- Measures
  Unique identifier for the mitigating control.

- Reduce significance
  When the mitigating control is implemented, this value is used to reduce the risk of rule violations. Enter a number between 0 and 1.

- Description
  Detailed description of the mitigating control.

- Function area
  Assign a function area to the mitigating control.

- Department
  Assign a department to the mitigating control.

Additional Tasks for Mitigating Controls

You can apply several tasks to the mitigating control once the master data is entered. You obtain the most important information about a mitigating control from the overview form. In addition, in the task view, you can select the tasks described in the following.

Assign rules

Use this task to specify which compliance rule that mitigating control applies to. You can assign enabled and working copies of rules on this assignment form.

The mitigating controls that are assigned to the function definition to be tested, are automatically transfered to the SAP function rules. Conditions:

- Active rules are assigned to a functional area and a department.
- The function definitions to be tested are assigned to the same functional area and to the variable set associated with the same department.

Assign function Definitions

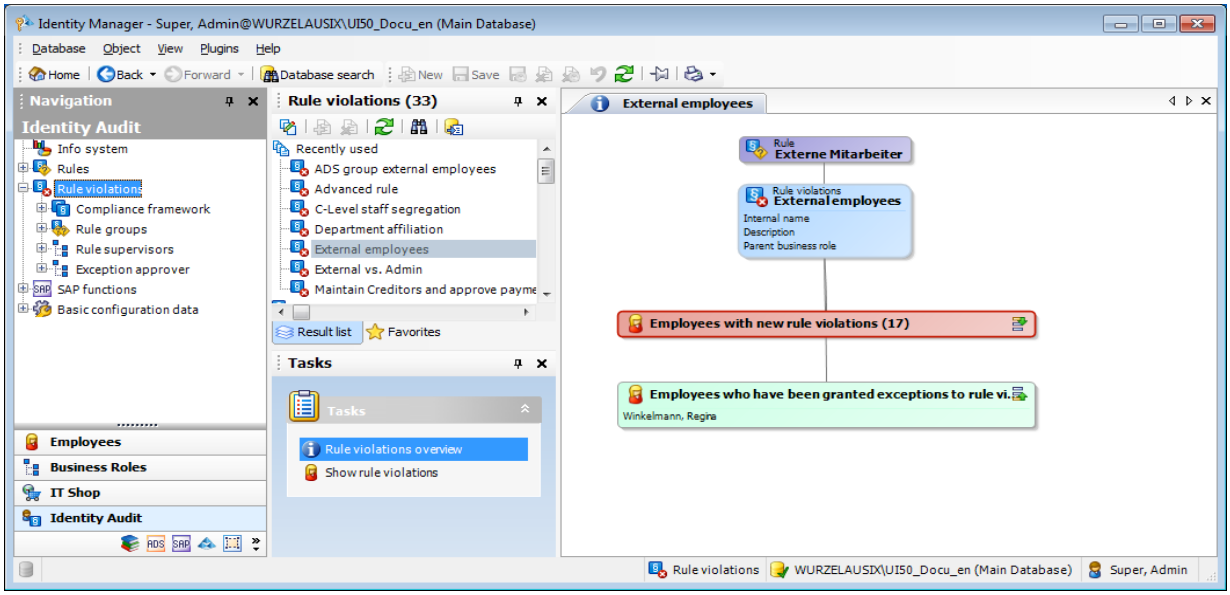
Use this task to specify the function definitions for which a mitigating control is valid. You can only assign function definitions that are enabled on the assignment form.

Rule Violations

For every rule in the Identity Manager there is a role added for the rule violation so that all employees that are found to violate the rule during a rule check can be allocated to exactly this rule. Therefore, every employee that violates a rule becomes a member of a role with the role class ”rule violation“. For more detailed information about roles and role classes refer to section Basic Data for Constructing Roles on page 84. Details of rule checking are described in the section Rule Checking on page 449 .

Rule violation are displayed in the category <Identity Audit>\<Rule violations>.

Rule Violations



Setting up and Editing Rules

Rules are never created and edited directly. You should always using a working copy. The changes to the rule do not take effect until the working copy is enabled. The rules and their working copies are displayed in the category <Identity Audit>\<Rules>.

Adding a New Rule

A working copy is created when a new rule is added. Once you have added all the data, you enable the working copy with the task <Enable working copy>. The rule is not added to the database until the working copy is enabled. The copy remains and can be used for making changes to the rule later. A role for rule violations is also added automatically when a new rule is created. The employees that violate this rule are added to the role.

Working with an Existing Rule

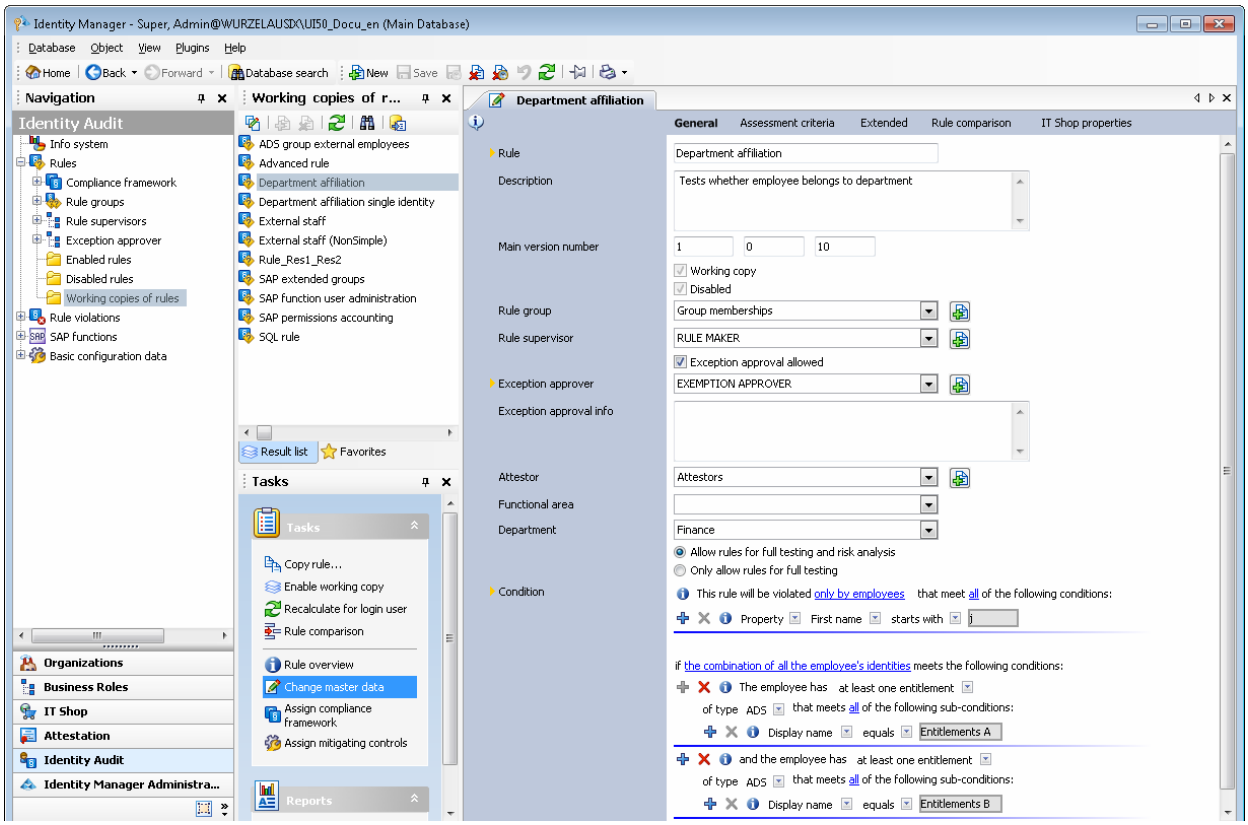
Existing rules are always edited with the working copy. Run the task <Create working copy> for the rule in order to do this. The data from the existing working copy is overwritten by the data from the original rule on request. The working copy is opened and can be edited. After saving the copy, you transfer the changes to the rule using the task <Enable working copy>. This prompts the rule to be enabled and puts it into action.

The Identity Manager users with the application role <Identity Audit>\<Rule supervisor> can edit existing rules if they are entered as a rule supervisor in the general data.

General Master Data for a Rule

Enter master data for a rule on the working copy master data form. Take care to fill out all compulsory fields

Setting Up a Rule



You need to enter at least the following data for a rule:

- Rule
  When you enter a name for a new rule, a role for rule violations is automatically created. All employees that violate this rule are added to the role.

When you rename a compliance rule, the names of associated rule violations are not changed.
Create a custom process to transfer changes from compliance rules (column ComplianceRule.Ident_ComplianceRule) to the associated rule violations (column NonCompliance.Ident_NonCompliance).

- Condition
  This is where you specify which conditions lead to a rule violation. You enter conditions using a Rule Editor. The condition is internally defined as a valid database query WHERE clause. Refer to the section Creating Rule Conditions on page 439 for more information.

Other rule data is:

- Working copy
  If this option is set, the rule is a working copy.

- Disabled
  Labels whether the rule in active use or disabled.
  Only rules that are enabled are included in rule checking. Use the tasks <Enable rule> or <Disable rule> to enable or disable rule. A rule's working copy is always disabled.

- Rule description
  The description should be used to describe the rule from a non-technical point of view.

- Rule groups
  Use rule groups to group rules by functionality, for example, to group account policies or separate functions ("Segregation of duties").

- Rule supervisor
  Select an application role from the <Identity Audit>\<Rule supervisor> drop-down menu. All employees that are assigned to this application role are responsible for the content of this rule. This may be an auditor or a auditing department, for example. Rule supervisors can edit and enable working copies of rules that they are assigned to in Identity Manager. Read the section Maintaining the Rule Supervisor and Exception Approvers on page 432 for information about setting up the application role and registering the employees responsible.

- Exception approver allowed
  Specify whether exception approval is permitted when a rule is violated. Assignments or requests that violate the rule can therefore be approved and issued anyway.

- Exception approver
  Select an <Identity Audit>\<Exception approver> application role from the drop-down menu. If rule violations are found, all employees assigned to this application role can grant exception approval for requests or assignments affected by this rule. Read the section Maintaining the Rule Supervisor and Exception Approvers on page 432 for information about setting up the application role and registering the employees responsible.

- Exception approval info
  Enter the information that the exception approver needs to make a decision.
  This advice should describe the risks and side effects of an exception.

- Attestor
  Specify the application role that employees with approval permission are deteremined from in an attestation procedure. For more information read section Attestation Approval Procedures on page 475.

- Functional area
  Assign a functional area that is relevant for the rule.

- Department
  Assign a department that is relevant for the rule.

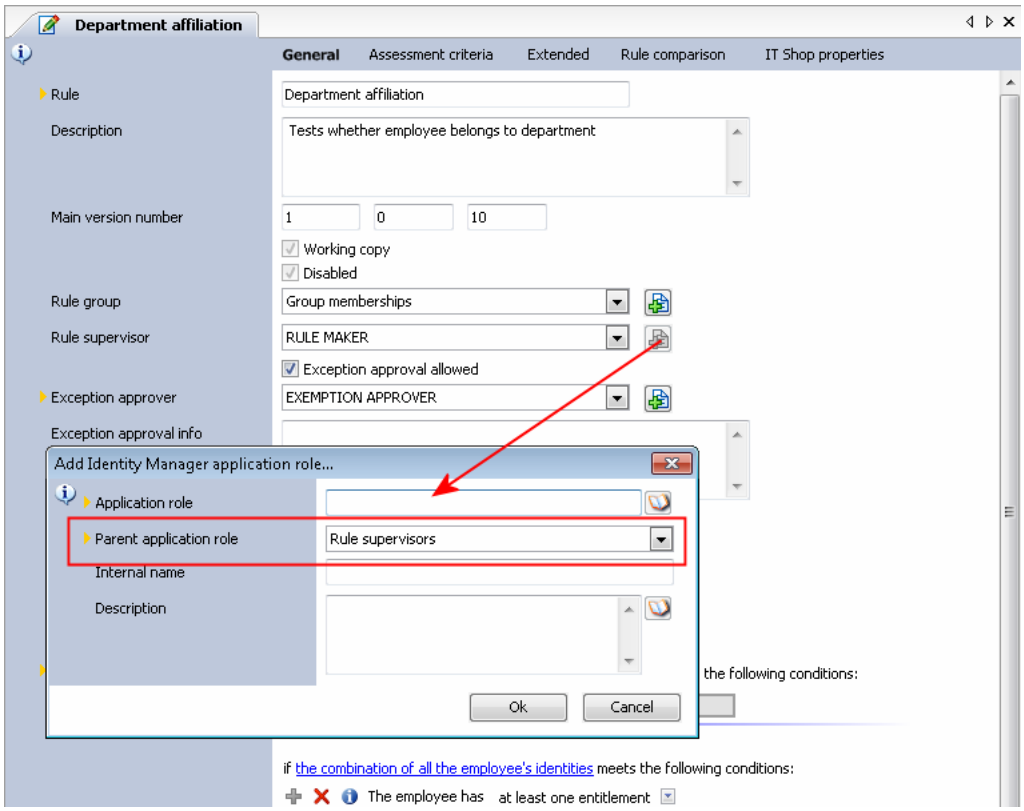
- Main version number
  The version number should mirror the rule's status. The version number consists of the main version number, the subversion number and the update version number. In the Identity Manager's default installation the version number is automatically incremented when changes are made to the rule condition.

Maintaining the Rule Supervisor and Exception Approvers

The default installation supplies both the Identity Manager application roles, "rule supervisor" and "exception approver". You can add rule supervisors and exception approvers to these. You may set up other application roles a level below this for rule supervisors and exception approvers, if required.

Create new application roles for rule supervisors or exception approver on the master data working copy form. To do this, use the ”insert“ button next to the corresponding input field.

Entering A New Application Role for a Rule Supervisor



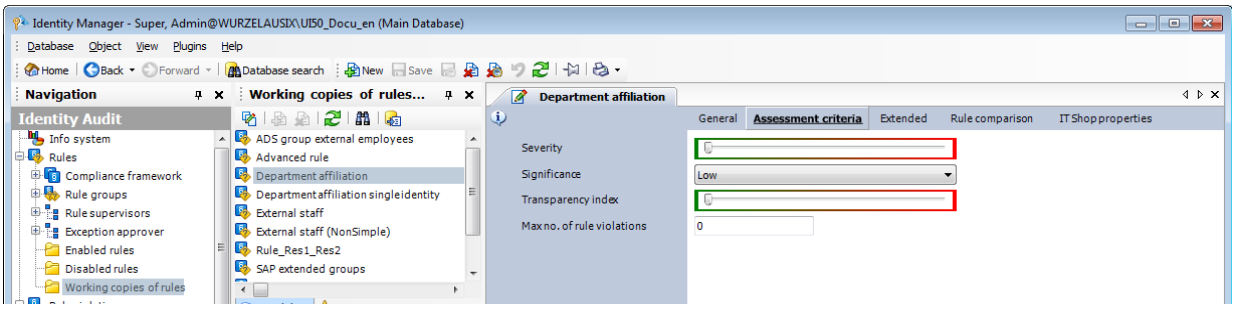
Enter at least one name for the application role. A new rule supervisor application role has to have the parent role ”Rule supervisor“. A new exception approver application role must have the application role ”Exception approver“as parent. Then edit the other data for the application role in the category <Identity Manager Administration>\<Identity Audit> in Identity Manager. To do this you need to log in with a role based authentication mode from the application role <Identity Audit>\<Administrators>. After you have specified the application roles, assign a manager to them. Refer to section How to Edit Identity Manager Application Roles on page 67 for more information.

If you working with the Manager, assign a supervisor to the selected application roles using the tasks available for this rule. These are <Maintain exception approver> and <Maintain rule supervisor>.

Rule Assessment Criterion

To evaluate the risk of a rule violation in the context of identity audit, you can enter values for grading rules at this point.

Enter Assessment Criteria for a Rule



- Severity
  Specifies the impact on the company of violations to this rule. Enter a value between 0 and 1
  0 ... no impact
  1 ... every rule violation poses a problem.

- Significance
  Provides a verbal description of the impact on the company of violations to this rule. In the default installation value list is displayed with the entries { NONE, 'low', 'average', 'high', 'critical'}.

- Risik index
  Specifies the risk for the company of violations to this rule. Enter a value between 0 and 1.
  0 ... no risk
  1 ... every rule violation poses a problem.
  For more information read section Risk Evaluation on page 427

- Transparency index
  Specifies how traceable assignments are that are checked by this rule. Enter a value between 0 and 1.
  0 ... no transparency
  1 ... fully transparency

- Max. no. of rule violations
  Specifies how many rule violation are allowed for this rule.

Extended Rule Input

Extended master data includes additional comments about the rule and revision data. Enter the following on the <Extended> tab:

- Rule number
  You can also add a rule to identify the rule.

- Implementation notes
  You can use implementation notes to enter technical or contents explanations about the rule condition.

Audit data for the rule:

- State
  State of rule with respect to its audit state.

- Auditor
  Person that last took an audit.

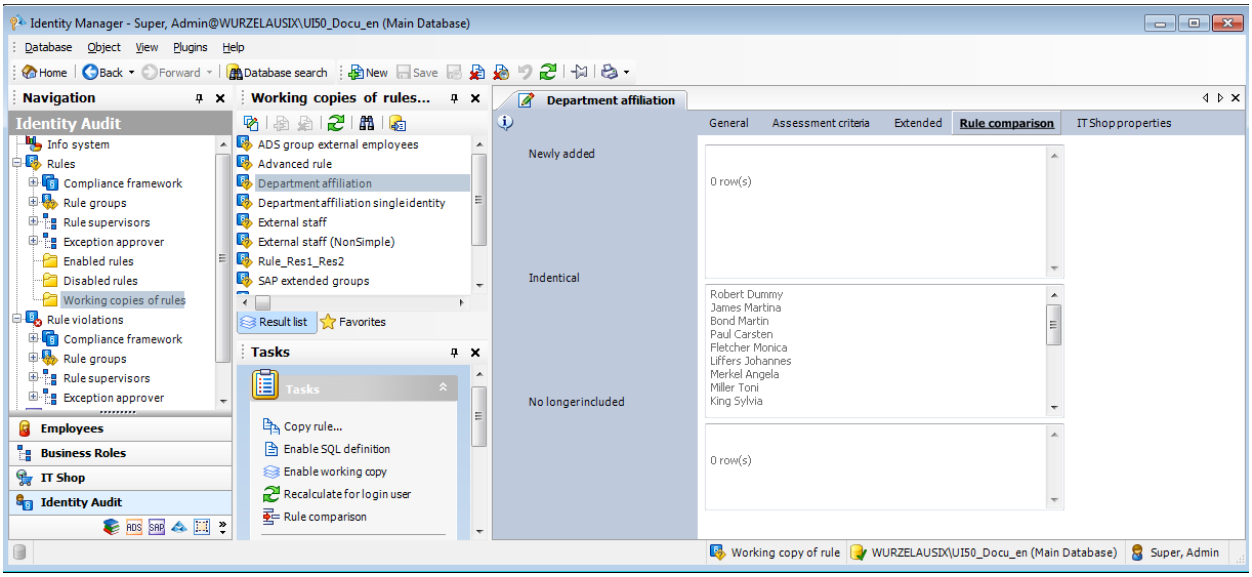
- Audit date
  Date of the last audit.

- Audit remarks
  Remarks refering to the audit, i.e. results that might be important for the next audit.

Comparing a Rule Working Copy with the Original

You can compare the results of a working copy with the original rule. To do this, run the task <Rule comparison> on the working copy. The comparison values are then displayed on the <Rule comparison> tab on the master data form.

Results of a Rule Comparison



The following values are determined:

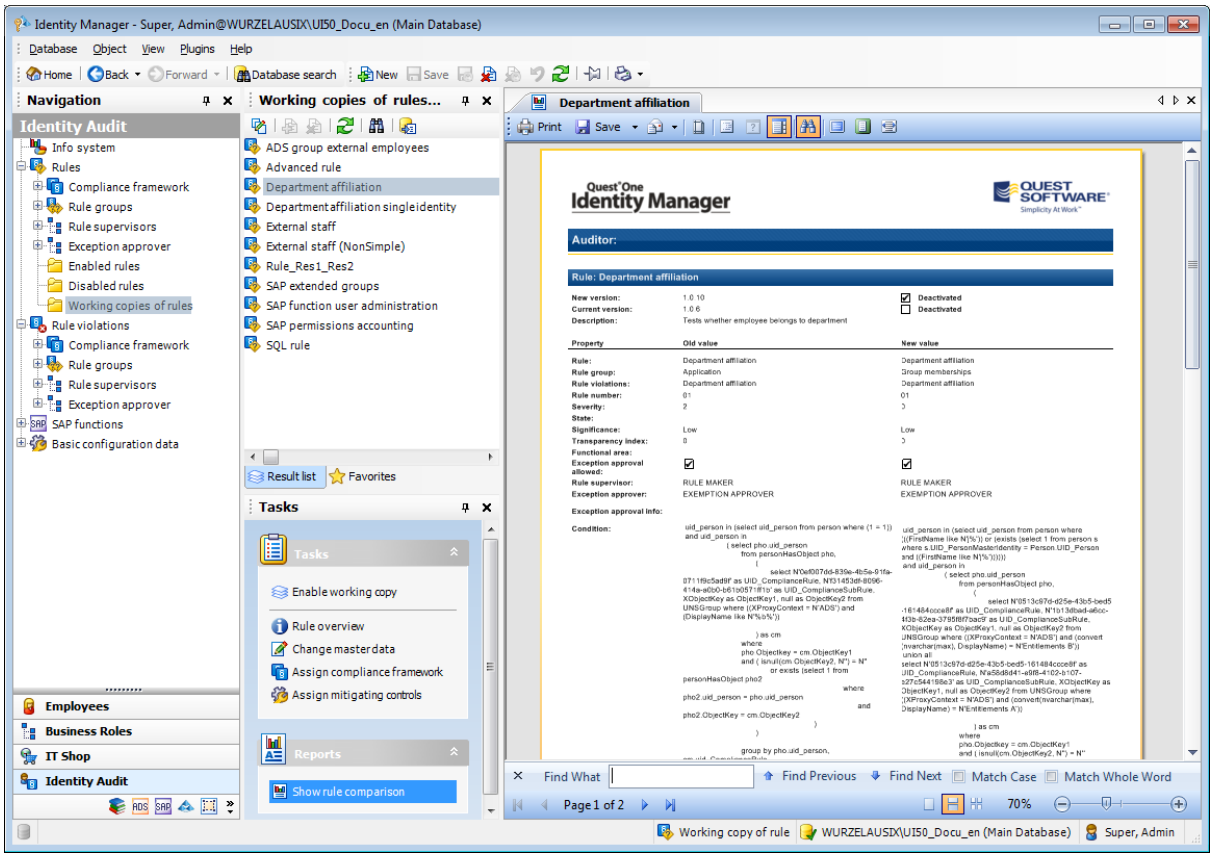
- Newly added
  Lists employees that are violating the rule for the first time due to changes made.

- Identical
  Lists employees that continue to violate the rule despite the changes.

- No longer included
  Lists the employees that no longer violate the rule due to the changes.

The comparison of the working copy with the original can also be presented in a report and saved. Use the task <Show rule comparison> to do this.

Displaying the Rule Comparison as a Report



IT Shop Properties for a Rule

Configuration Parameter for IT Shop Relevant Properties

CONFIGURATION PARAMETER	MEANING WHEN ACTIVE
QER\ComplianceCheck\EnableITSettingsForRule	IT Shop properties for the compliance rule are visible and can be edited.

The tab <IT Shop properties> is only shown if the configuration parameter ”QER\ComplianceCheck\EnableITSettingsForRule“ is set. Specify how violations of this rule should be handled within an IT Shop approval process.

Specify which violation should be logged for the rule by using the IT Shop property <Rule violation identified>. The following values are permitted:

- New rule violations due to requesting
  Only rule violations that would arise by approving the current request are logged.

- Unapproved exceptions
  Rule violations that would arise by approving the current request are logged. Already known rule violations that have not yet been granted an exception are also logged.

- All compliance violations
  All rule violations are logged without taking into account whether exception approval has been granted or not.
  This value is automatically set when the option <Explicit exception approval> is enabled.

Use the IT Shop property <Explicit exception approval> to specify whether the reoccurring rule violation should be presented for exception approval or whether an existing exception approval can be reused.

- If the option is set, a known rule violation must always be presented for exception approval, even if there is an exception approval from a previous violation of the rule.

- If the option is not set, a known rule violation is not presented for exception approval again if it already has exception approval from a previous violation. This exception approval is reused and the known rule violation is automatically granted exception.

If several rules are violated by a request and <Explicit exception approval> is set for one of the rules, the request is presented for approval to all exception approvers for this rule.

Rules that have the option <Explicit exception approval> set, result in a renewed exception approval if:

- A rule check is carried out within the approval process for the current request and

1. the rule is violated by the current request
   or

2. the IT Shop customer has already violated the rule.

In case 1) the request for the IT Shop customer is presented to the exception approver. If the request is approved, case 2) applies to the next request. In case 2), every request for the IT Shop customer must be decided by the violation approver, even when the request itself does not result in a violation. The result you acheive is that assignments for employees that have been granted an exception, are verified and reapproved for every new request.

There are two scheduled tasks supplied with the default installation for checking rules. These scheduled tasks are assigned by default to every rule via the input fields <Test schedule> and <Fill schedule>. Here you can assign custom schedules. Refer to section Rule Checking on page 449 for more details about schedules.

Additional Tasks for Rules

Once the master data for a rule have been entered you can apply different tasks to it. The overview form provides the most important information about a rule. In addition, in the task view, you can select the tasks described in the following.

Assign Compliance Framework

Compliance frameworks are used to classify rule according to regulatory requirements such as internal requirements, auditing requirements or SOX requirements. Use the task <Assign compliance framework> to specify which compliance frameworks are relevant for the selected rule.

Assign Mitigating Controls

The risk of rule violations can be reduced by suitable control measures. For example, the risk associated with this rule violation can be reduced by regular manual checking of invalid entitlements. Read section Setting up Mitigating Controls on page 428 about how to set up mitigating controls. Use the task <Assign mitigatin controls> to specify which mitigating controls apply for the selected rule.

Enable/Create Working Copy

Use the task <Enable working copy> to create a new working copy of rule. If you apply the task to an exisiting working copy, the changes are transfered to the rule.

To change an existing rule, run the task <Create working copy>. The data from the existing working copy are overwritten by the data from the original rule after a security prompt.

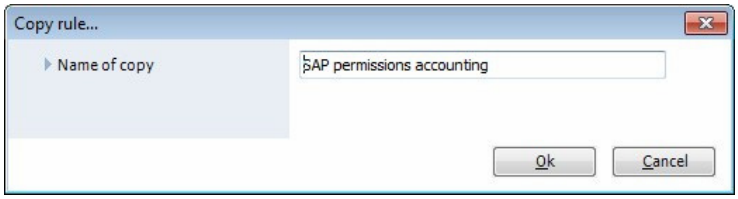
Recalculate...

There are several tasks available for immediately checking a rule. The effect of these tasks is explained in the section Rule Checking on page 449.

Copy rule...

Use the task <Copy rule...> to create a copy of the selected rule. This opens a dialog window where you can enter a name for the copy.

Copy Rule Dialog Window



Copy the rule with the <OK> button. This creates a working copy with the givenname.

The Identity Manager asks you whether you want to edit the copy immediately. If you confirm the prompt with the <Yes> button, the master data form is opened and you can edit the data straight away. If you want to edit the working copy at a later date, close the prompt with the <No> button.

Rule Comparison

If you have made changes to the rule condition in a working copy, you can determine the effects of this via a comparison with the original rule. Rules can only be compared when an original of the working copy exists. Refer to section Comparing a Rule Working Copy with the Original on page 435 for more information.

Enable/Disable Rule

Enable the rule so that rule violation can be found. That is why there is a task <Enable rule> for disabled rules. To exclude rules from testing, you can disable them. Use the task <Disable rule> for enabled rules. Any existing memberships in the associated rule violation role are removed by the DBScheduler. The working copy rule is always disabled.

Enable SQL Definition

If the configuration parameter ”QER\ComplianeCheck\PlainSQL“ is enabled, you can formulate the rule condition directly as an SQL query in advanced mode. To do this, run the task >Enable SQL definition>.

Creating Rule Conditions

Configuration Parameter for Advanced Mode

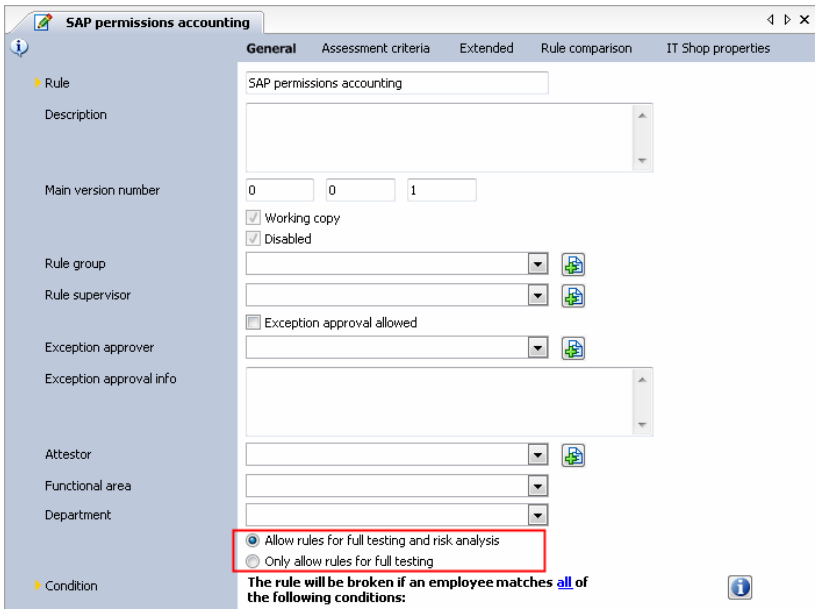
CONFIGURATION PARAMETER	MEANING WHEN ENABLED
QER\ComplianceCheck\SimpleMode\NonSimpleAllowed	Rules can be created in advanced mode

Use a rule condition to describe the restrictions required to fulfill a rule. There are two ways to define rule conditions:

1. Simple definition
   The affected employee group and assignments are restricted separately in the rule condition. Employees that the rule condition will be applied to are determined via the employee group. The properties are defined via the affected assignments that result in a rule violation for the affected employees. The assignments are determined via the object relations of the affected employees (table ”PersonHasObject“).
   The simple definition is used as default to create rule conditions. It is available when the configuration parameter QER\ComplianceCheck\SimpleMode\NonSimpleAllowed and the option <Allow rules for full testing and risk analysis> are set.

2. Advanced mode
   Employee properties are defined in the rule condition that lead to a rule violation. The assignments are determined directly by the respective base tables, which contain the selected objects (e.g. ”PersonHasSAPGRoup“ or ”Person“).
   Advanced mode is only available when the configuration parameter QER\ComplianceCheck\SimpleMode\NonSimpleAllowed is enabled and the option <Only allow rules for full testing> is not. Refer to section Creating Advanced Rule Conditions on page 445 for more information.

Options for Rule Conditions



You cannot return to the simple definition once a rule condition has been entered in advanced mode!

You can integrate checking of requests for rule compliance into approval workflows in IT Shop. The Identity Manager provides two approval procedures for this. Compliance rules that have been created in advanced mode are only to taken into account if the approval procedure ”CC“ is used in the approval worlkflow. The approval procedure ”CR“ only takes into account compliance rules that have been created via simple definition mode. See the section Testing Requests for Rule Compliance on page 68 in the IT Shop Manual for more information.

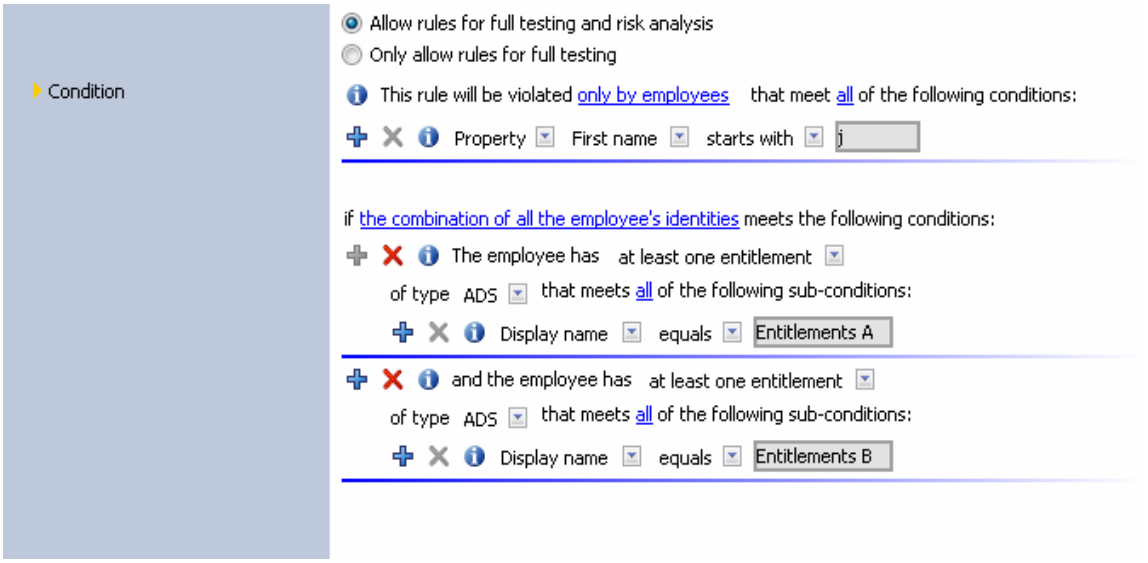
Basics for Using the Rule Editor

Configuration Parameters for Entering Extended Rule Conditions

CONFIGURATION PARAMETER	MEANING WHEN ACTIVE
QER\ComplianceCheck\Simple-Mode\ShowDescriptions	Displays additional input fields for describing the compliance rules in the Rule Editor.

The Rule Editor is there to help you formulate rule conditions. Inputting the rule condition is eased by predefined condition types and by limiting valid operators. The completed database query is put together internally. If the configuration parameter QER\ComplianceCheck\SimpleMode\NonSimpleAllowed is enabled, additional input fields are displayed providing a more detailed description of each rule block..

Rule Editor for Simple Definition of Rules


Condition
Allow rules for full testing and risk analysis
Only allow rules for full testing
This rule will be violated only by employees that meet all of the following conditions:
Property First name starts with j
if the combination of all the employee's identities meets the following conditions:
The employee has at least one entitlement
of type ADS that meets all of the following sub-conditions:
Display name equals Entitlements A
and the employee has at least one entitlement
of type ADS that meets all of the following sub-conditions:
Display name equals Entitlements B

The Rule Editor control elements supply operators and properties that you need to formulate partial conditions. Select one entry from the simple pop-up menu. In certain extended pop-up menus where the properties are displayed hierarchically, you can select several entries together. These are linked with an ‘OR’ in the condition. You may enter text directly into input fields. Pop-up menus and input fields are shown and hidden dynamically.

A rule condition is made up of several rule blocks. A rule violation is detected when an employee, with properties and assignments, can be matched to all the rule blocks.

There are two types of rule blocks:

- Affected groups of employees
  Each rule must obtain exactly one rule block that specifies the employee group that the rule should be applied to. By default, all employees are taken into account. You can, however, restrict the employee groups more.

- Assignments affected
  You need to define at least one rule block that finds affected assignments. The properties that lead to a rule violation in the employee group affected are defined here. You can check the following assignments in the rule block: roles, target system groups, system entitlements, system roles, applications, resources.

If requests are tested for rule compliance in IT Shop, all objects that are found via a rule block for the affected assignments lead to a rule violation. If an employee becomes a member of an affected group of employees via a request in IT Shop, the rule violation is not discovered until the request is approved and the company resource or role is assigned. This means: every assignment that should be detected by testing for rule violations, must be defined in the rule block for the affected assignments.

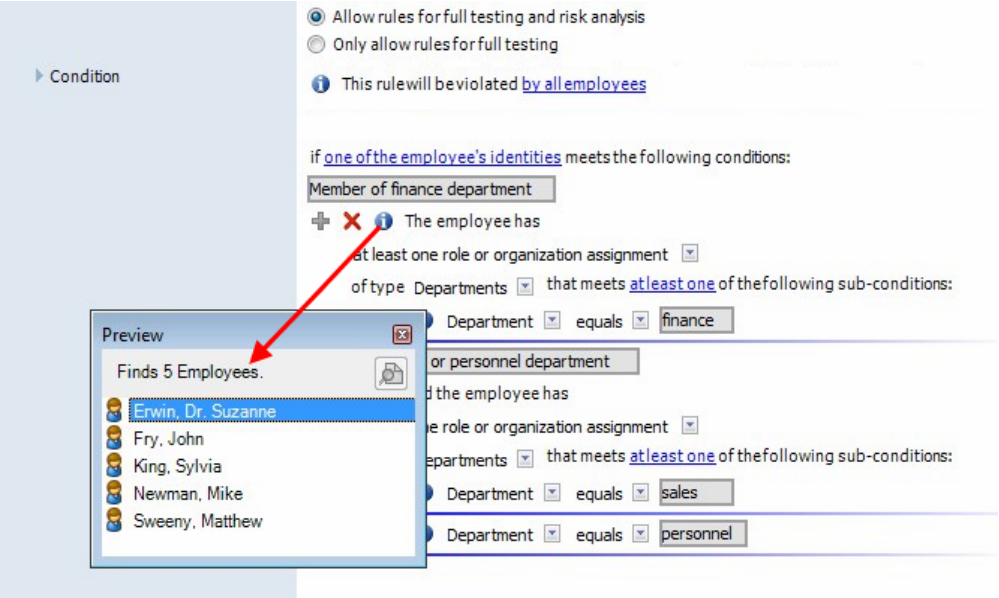
You can add any number of partial conditions within one rule block and link them with each other. Use the options <All> and <At least one> to specify whether one or all partial conditions in the block have to be fulfilled.

Meaning of Icons in the Rule Editor

ICON	MEANING
	Add another partial condition or another rule block. A new line is displayed for entering the condition.
	Delete the partial condition or rule block. The line is removed.
	Opens the preview window. All affected employee objects are shown.

In the preview, you can see the employee objects affected in a single partial condition or the complete condition. The number of affected employee objects is display in the preview window's header. Use the icon in the preview window header to hide and show the affected employee objects.

Preview


Allow rules for full testing and risk analysis
Only allow rules for full testing
Condition
This rule will be violated by all employees
if one of the employee's identities meets the following conditions:
Member of finance department
The employee has
at least one role or organization assignment
of type Departments that meets at least one of the following sub-conditions:
Department equals finance
Preview
Finds 5 Employees.
Erwin, Dr. Suzanne
Fry, John
King, Sylvia
Newman, Mike
Sweeny, Matthew
or personnel department
the employee has
role or organization assignment
epartments that meets at least one of the following sub-conditions:
Department equals sales
Department equals personnel

Specifying the Affected Employee Group

Each rule has to contain exactly one rule block which specifes the employee group. The following options are available for specifying employee groups in the Rule Editor:

- From all employees
  If this option is set, all employees are taken into account.

- Only from employees that fulfill all/at least one of the following conditions
  If this option is set, you can limit the employee group more, for example, "All employees in group A" or "All external employees". To determine the affected employee group, formulate the appropriate partial condition.

You can specify a condition type in the first pop-up menu of the partial condition which restricts the affected employee group.

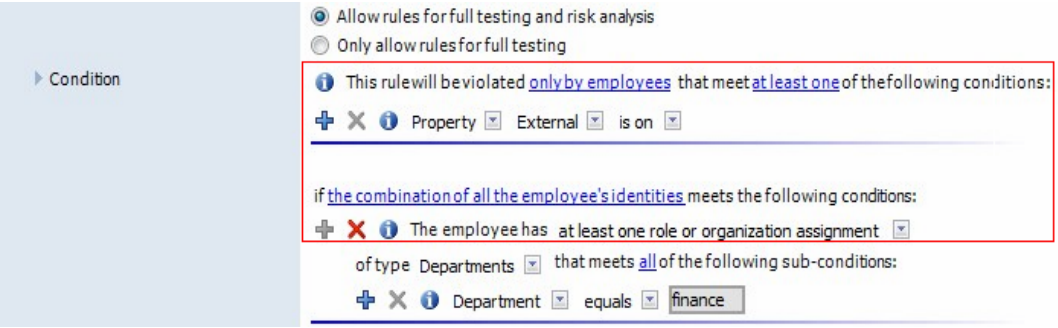
Valid Condition Types in the Rule Editor

CONDITION TYPE	MEANING
Property	Employee object properties. The valid properties pop-up menu is already limited to the most important of the employee's properties.
User account in	Employee's user account. The valid user account properties depend on the selection of the target system and the target system area.
SQL Query	Input of an SQL condition (WHERE clause).

You can specify, for each rule individually, whether they should be valid on a between identities or on an identity specific basis. This is particulary important if you are working with employees that have main and sub identities. By default, a rule is valid for all of an employee's identities, that means any rule violations that are found are associated with the main and sub identities of an employee. If the rule violation should only be assigned to the employee's subidentity, then formulate the rule for a single iden-

tity of that employee. Read section Mapping Multiple Employee Identities on page 58 on how to use several identities for an employee.

Rule Block for the Employee Group Affected


Condition
Allow rules for full testing and risk analysis
Only allow rules for full testing
This rule will be violated only by employees that meet at least one of the following conditions:
Property External is on
if the combination of all the employee's identities meets the following conditions:
The employee has at least one role or organization assignment
of type Departments that meets all of the following sub-conditions:
Department equals finance

Specifying Affected Assignments

Configuration Parameter for Hiding Target System Groups

CONFIGURATION PARAMETER	MEANING WHEN ENABLED
QER\ComplianceCheck\SimpleMode\HideNamespaces	Assignments of type resource, application, system role as well as target system types mapped in Unified Namespace can be selected. Target system groups that are directly mapped in the Identity Manager data model are hidden.

In order to take assignments into account in the rule, you have to define at least one rule block that contains the assignments that are affected. Localize these assignments via the options:

- At least one entitlement
  Define only one entitlement per rule block.

- Combinations of entitlements
  Here you need to define at least two entitlements that have one common extended property or belong to one property group. A condition without extended property data is not permitted here.

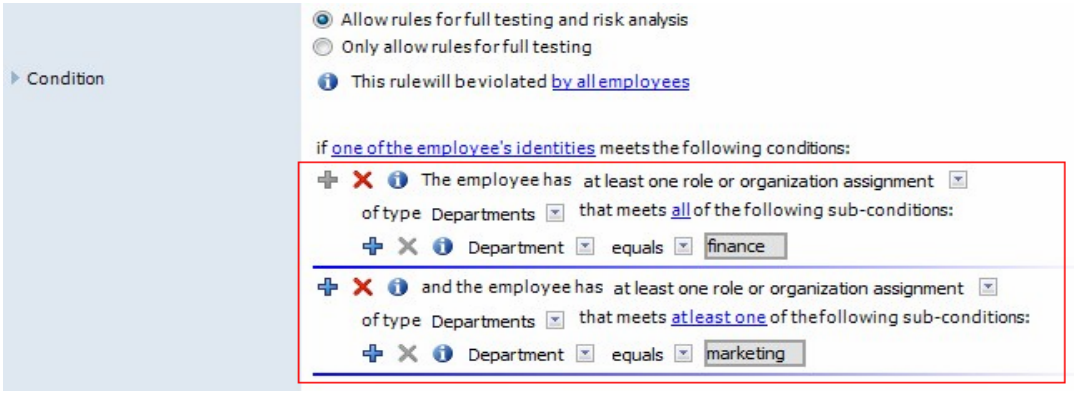
- At least one functions
  Enter at least one SAP function that will be violated by the rule.

- At least one role or organization assignment
  Define one role class assignment per rule block (Identity Manager application roles, departments, locations, cost centers, business roles).

In this context, the term ”entitlement“ refers to company resources that are available to an employee. This includes group memberships in target system as well as system roles, applications or resources. First you secify the assignment type that should be tested, for example, ADS groups, resources or business roles. Then you can restrict the affected assignments further via one or more partial conditions. When you want to test assignment to target system groups that are directly mapped in the Identity Ma-

nager database, disable the system configuration parameter QER\ComplianceCheck\SimpleMode\HideNamespaces. The target system are also shown in the assignment types drop-down menu.

Rule Block for Affected Entitlements


Condition
Allow rules for full testing and risk analysis
Only allow rules for full testing
This rule will be violated by all employees
if one of the employee's identities meets the following conditions:
The employee has at least one role or organization assignment
of type Departments that meets all of the following sub-conditions:
Department equals finance
and the employee has at least one role or organization assignment
of type Departments that meets at least one of the following sub-conditions:
Department equals marketing

If the affected assignments are in several rule blocks, then a rule violation is acknowledged when an employee in the affected employee group is assigned least one object in all of the rule blocks. Rules that test a combinaton of entitlements with common extended properties always have two entitlements that only cause a rule violation in this combination.

A Simple Rule Example

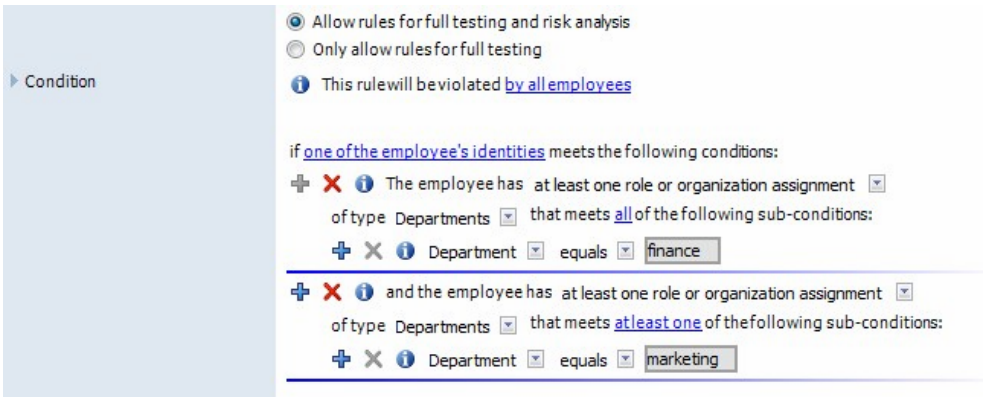
The following example is designed to show how rules can be created with the help of the Rule Editor and the effects of each option.

Rule 1: Employees from department A may not belong to department B at the same time.

Define:

1. the option <by all employees> in the rule block for all employee groups
2. two rule blocks for the affected assignments with the option <at least one role or organization>.

Rule Condition for Rule 1


Condition
Allow rules for full testing and risk analysis
Only allow rules for full testing
This rule will be violated by all employees
if one of the employee's identities meets the following conditions:
The employee has at least one role or organization assignment
of type Departments that meets all of the following sub-conditions:
Department equals finance
and the employee has at least one role or organization assignment
of type Departments that meets at least one of the following sub-conditions:
Department equals marketing

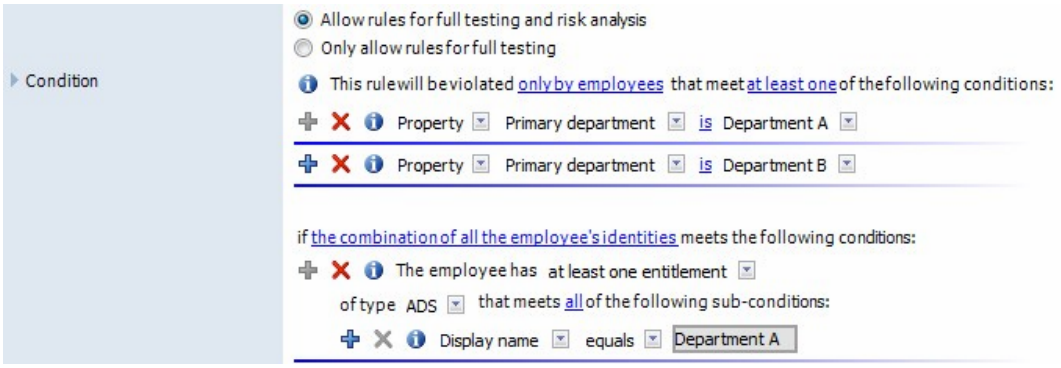
Rule 2: Employees that belong to department A or B may not access the Active Directory group "Permission A".

Define:

1. the option <only by employees> and <at least one> in the affected employee group in the rule block,

2. a rule block for the affected assignments with the option <at least one entitlement>.

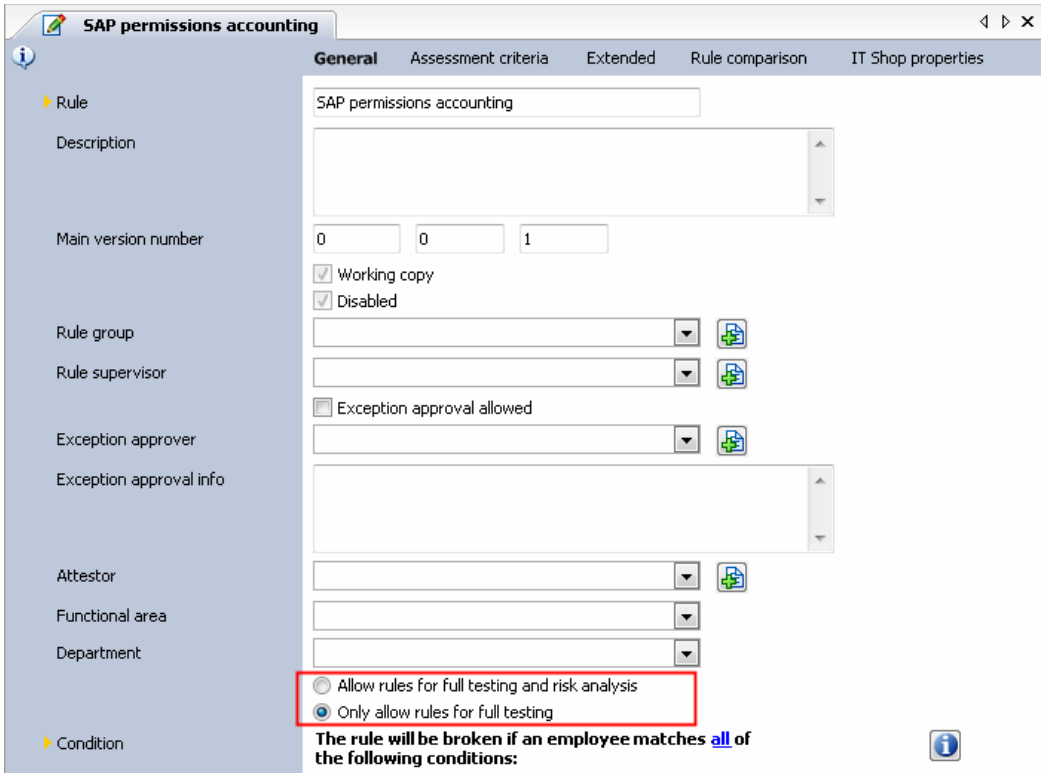
Rule Condition for Rule 2


Condition
Allow rules for full testing and risk analysis
Only allow rules for full testing
This rule will be violated only by employees that meet at least one of the following conditions:
Property Primary department is Department A
Property Primary department is Department B
if the combination of all the employee's identities meets the following conditions:
The employee has at least one entitlement
of type ADS that meets all of the following sub-conditions:
Display name equals Department A

Creating Advanced Rule Conditions

In order to create rules in advanced mode, enable the configuration parameter ”QER\Compliance-Check\SimpleMode\NonSimpleAllowed“. Then, the option <Allow rules for full testing and risk analysis> is additionally shown on the master data form when a rule is being created or set up. To swap to advanced mode enable the option <Only allow rules for full testing>. After confirming the security prompt the Rule Editor is displayed with a different interface

Changing to Advanced Mode for Rule Conditions



After entering a rule condition in advanced mode you cannot revert to the simple mode definition!

Rule conditions in advanced mode are based on the base object ”Personen“ (Table ”Person“). The completed database query is put together internally:

```
Select Firstname, Lastname from Person where
<Rule condition>
order by 1,2
```

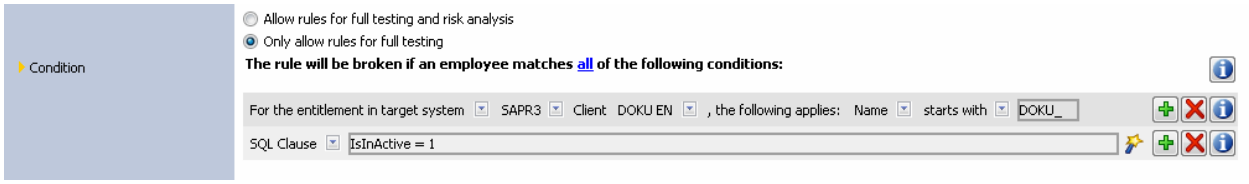
First you need to specify whether one or all of the following conditions have to be met in advanced mode. Specify the condition type in the first drop-down menu in the condition.

Valid Condition Types in Advanced Mode

CONDITION TYPE	MEANING
Property	Employee object properties. The drop-down menu with permitted properties is already restricted to the most important employee properties.
For the account in target system	Employee user account. Valid user account properties depend on which target system and target system area are selected.
For the entitlements in target system	Employee target system group. Valid group properties depend on which target system and target system area are selected.
SQL clause	Free chioce of SQL query (WHERE clause). The input can be entered directed or by using a wizard.

You have the possibility to link several conditions. Only ”and” is supported here as link operation.

Advanced Mode Condition



All other control elements that you need for formulating a condition are provided by operators and properties. You can only select one entry from the drop-down menu. You can select more entries from extended drop-down menus, where the properties are displayed hierarchically and then added to the condition using an ”or“ operator. Input of your won text is permitted via input fields. The valid input fields and drop-down menus are displayed dynamically.

Rule Conditions for SAP Functions

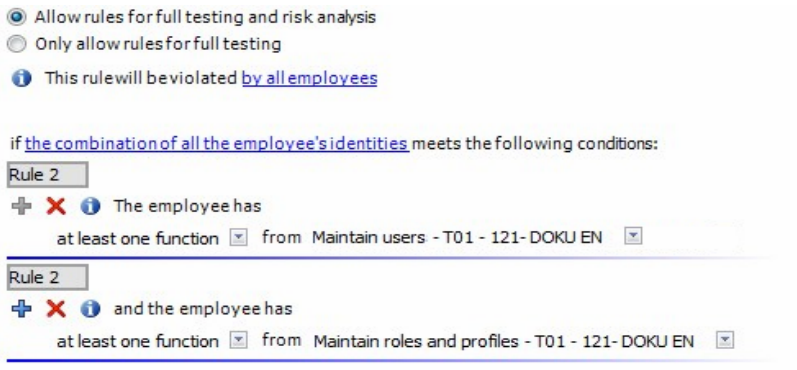
Configuration Parameters for Using SAP Functions

CONFIGURATION PARAMETER	MEANING
TargetSystem\SAPR3\SAPRights	Preprocessor relevant configuration parameter for controlling the model components for managing permissions within SAP R/3. If the parameter is set, the target system components are available. Changes to this parameter require recompiling the database.

Enable the configuration parameter TargetSystem\SAPR3\SAPRights in order to create rules about SAP functions and then compile the database.

Enable the option <Allow rules for full testing and risk analysis>on the rule's master data form so that you can define rule conditions for SAP functions. Limit the number of assignments effected with the option <At least one function>. If SAP authorizations in combination result in a rule violation, enter a rule block for each SAP function.

Condition for SAP Functions


Allow rules for full testing and risk analysis
Only allow rules for full testing
This rule will be violated by all employees
if the combination of all the employee's identities meets the following conditions:
Rule 2
The employee has
at least one function from Maintain users - T01 - 121- DOKU EN
Rule 2
and the employee has
at least one function from Maintain roles and profiles - T01 - 121- DOKU EN

When the Identity Manager tests rules, it finds all the employees whose assigned SAP users match the SAP functions that are given in the rule. An SAP user matches an SAP function when:

- An SAP role assigned to the SAP user matches the SAP function or
- An SAP role that is assigned a reference user that matches an SAP function and the SAP user is assigned this reference user.

Read the section User Account Login Data on page 369 on how to map reference userss. You can find detailed information about SAP functions in the section SAP Functions on page 456.

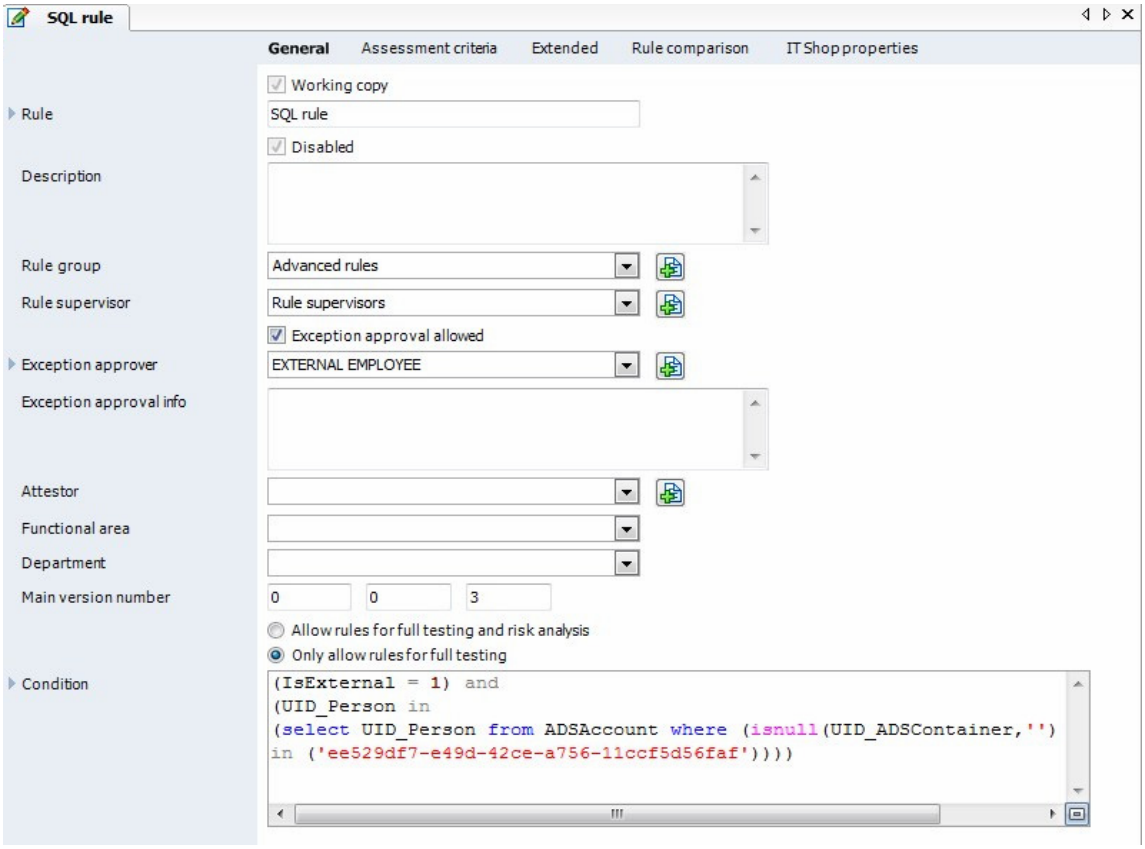
Rule condition as SQL query

Configuration Parameter for Entering More Rule Conditions

CONFIGURATION PARAMETER	MEANING WHEN SET
QER\ComplianceCheck\PlainSQL	SQL text is only permitted for rules in advanced mode.

If the parameter ”QER\ComplianceCheck\PlainSQL“ is set, you can formulate the rule condition directly in SQL. To do this, run the task <Enable SQL definition> on the working copy.

Direct SQL Query Input



Deleting Rule

All the information about a rule condition and rule violations is irrevocably deleted when the rule is deleted!
The data cannot be retreived at a later date.
Therefore, we advise you to write a report about the rule and its current violations before you delete it, if you want to retain the information (e.g. audit security).

A rule can be deleted when no rule violation exists for it (no employee is member rule violation role associated with the rule). Proceed as follows to delete rules:

- Disable the rule
  Run the task <Disable rule> on the rule to be deleted.
  Any existing memberships in the rule violation role associated with this rule are removed by the DBScheduler.

- Delete rule
  Once the DBScheduler has recalculated the violations for the rule, delete the rule using the appropriate icon in the Identity Manager or the Manager user interface.
  The rule, the associated rule violation role and the working copy are deleted.

Rule Checking

To test a rule, processing tasks are created for the DBScheduler. The DBScheduler determines in the case of each rule, which employees satisfy the rule and which employees violate the rule. Follow-up tasks ensure that those employees that violate the rule are entered in to the role provided for that purpose. The specified rule approvers can test rule violations and if necessary grant exception approval.

Checking a Rule

General Configuration Parameter for Rule Compliance

CONFIGURATION PARAMETER	MEANING
QER\ComplianceCheck\CalculateImmediately	Tasks for recalculating rule violations are immediately started when relevant change occur.

Rules are checked by using the analysis from object assignment auxilary tables. These tables are regularly updated by the DBScheduler. When changes are made to a rule, the auxilary tables are immediately recalculated. In the default installation of the Identity Manager there is a scheduled task ”default Schedule ComplianceRule Fill“ which can be used to include other changes in the rule check, such as, changing entitlements or changing extended properties. This task creates processes to update the auxilary tables on a cyclical basis. You can edit this scheduled task in the category <Identity Audit>\<Basic configuration data>\<Process schedules>.

The actual rule check is started using different methods. Only enabled rules are taken into account, that means that disabled rules are not processed!

The processing requests for rule checking are immediately generated when a rule is added, changed or deleted. All employees are checked to see if they fulfill the affected rule. The scheduled task ”default Schedule ComplianceRule Check“ is included in the Identity Manager’s default installation and checks the entire set of rules. This task creates a processing request for the DBScheduler on a regular basis. You can also edit this scheduled task in the category <Identity Audit>\<Basic configuration data>\<Process schedules>.

Calculation tasks can be initiated immediately or cyclically when changes are made to employee assignments or to user account group memberships. You can specify the interval between new calculation tasks with the configuration parameter ”QER\ComplianceCheck\CalculateImmediately.“ If the parameter is set, the tasks for recalculating rule violations are immediately run for the relevant changes. If the parameter is not set, the calculation tasks are executed the next time the scheduled task ”Default Schedule ComplianceRule Check“ is run.

There are different tasks available for rules in for immediate testing:

- Recalculate Rule
  All employees are checked to see if they comply to the current rule.

- Recalculate for login user
  The logged in user is checked for compliance to all rules.

- Recalculate all
  All employees are check for compliance to all rules.

When a rule is violated, the affected employee is added to the corresponding role for rule violations. You can rerun the tests on all the rules for these employees, Read the section Rule Checking on page 450 for more information.

For requests within IT Shop that go through an approval procedure with rule checking, customers are checked to see if they violate rules when their request is being approved. There could be several methods for checking rules in this case. More detailed information can be found in section Testing Requests for Rule Compliance on page 68 in the IT Shop Manual.

You can set up more scheduled tasks to regularly fill auxillary tables and to test individual rules. Ensure that the scheduled tasks are assigned to the the rules. To do this, run the tasks <Assign rule (for filling)> and <Assign rule (for testing)> on the scheduled tasks. Edit the schedules in the category <Identity Audit>\<Basic configuration data>\<Schedules>. Setting up and configuring scheduled tasks is described in more detail in the section Setting Up a Scheduled Task to Calculate Dynamic Roles on page 103 näher erläutert.

Rule Checking

Each rule points to its own application role for rule violations. Employees that violate a rule, are added to the role designated for the rule that is effected. There are two forms available for rule checking that are supposed to answer the following questions:

- Which employees violate a particular rule?
- Which rules are violated by a particular employee?

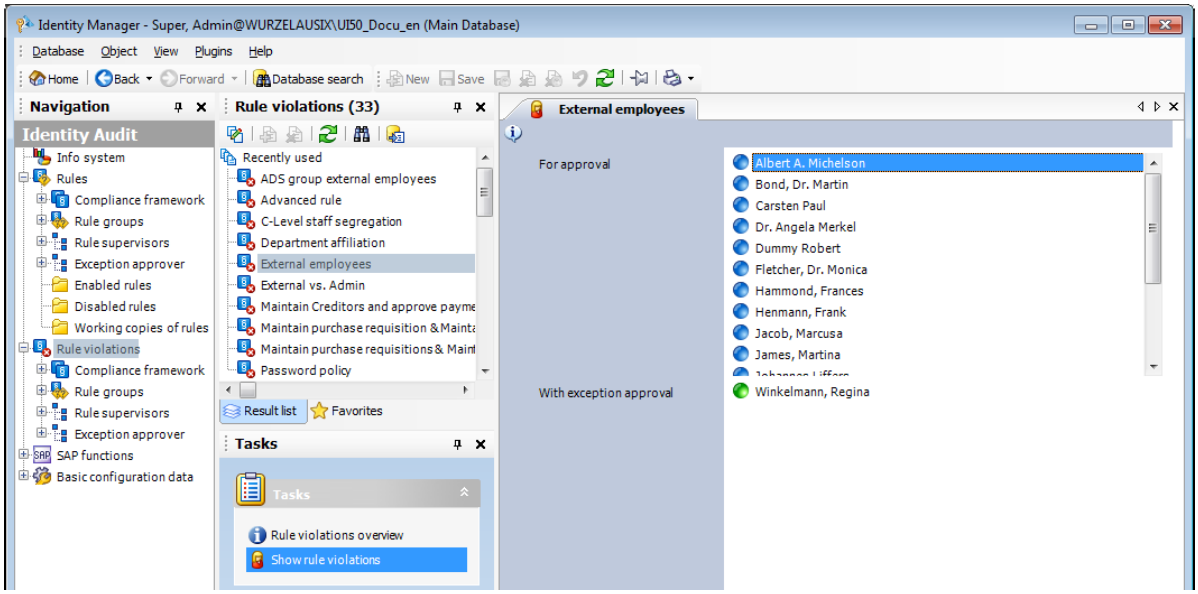
Which Employees Violate a Certain Rule?

Change to the category <Identity Audit>\<Rule violations> to find employees that have violated a rule. The roles for rule violation are displayed here. Select a rule violation from the list. Use the task <Show rule violations> to show all the employees that are members of the selected role for rule violations and have violated a certain rule. The form differentiates between:

- Employees pending a rule violation desicion
- Employees with exception approval

- Employees without exception approval

Rule Analysis



The icons on the form have the following meaning:

Meaning of Rule Evaluation Icons

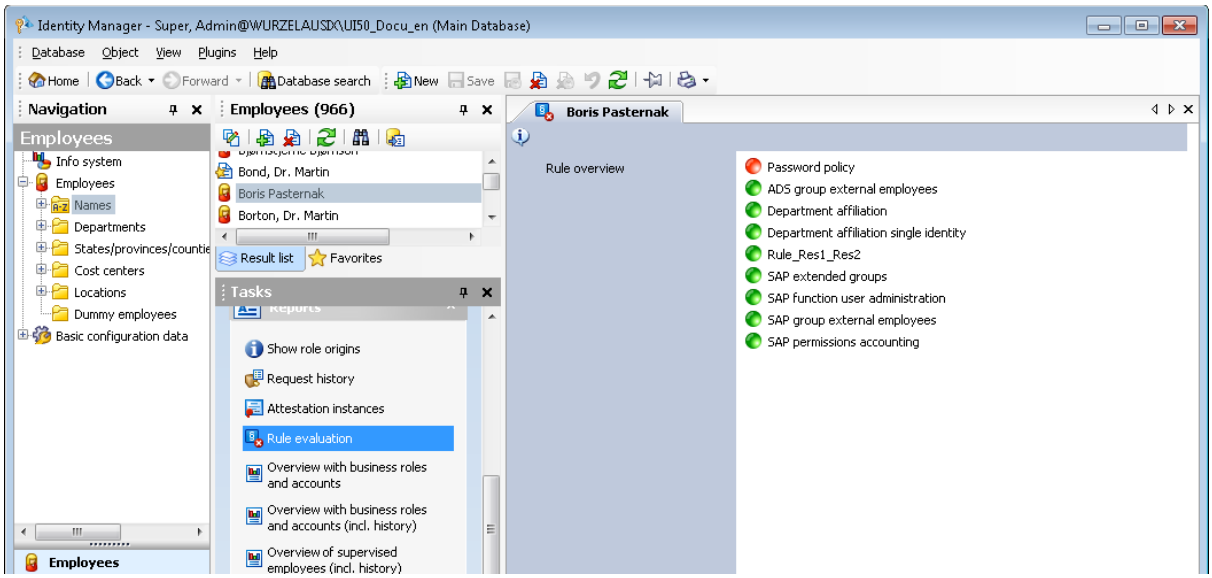
ICON	MEANING
	No rule violation. A violation has not yet been decided.
	Rule violation with no exception.
	Rule violation but an exception has been granted.

Which Rules are Violated by a Certain Employees?

To find out, which rule a particular employee has violated, select the employee in the category <Employee>\<Employees>. To do this, log in with a role based authenication model from the application role <Personen>\<Administrators>. You can also edit employee data in the Manager. Open the report

<Rule analysis> for the employee. This not only shows the rule that the employee has violated with or without exception, but also those with no violations.

Employee Rule Evaluation



The icon on the form have the following meaning:

Meaning of icons in Employee Rule Analysis

ICON	MEANING
	No rule violation exists.
	There is a rule violation. No exception approval has been granted for this rule exception.
	There is a rule violation which has been granted exception approval.

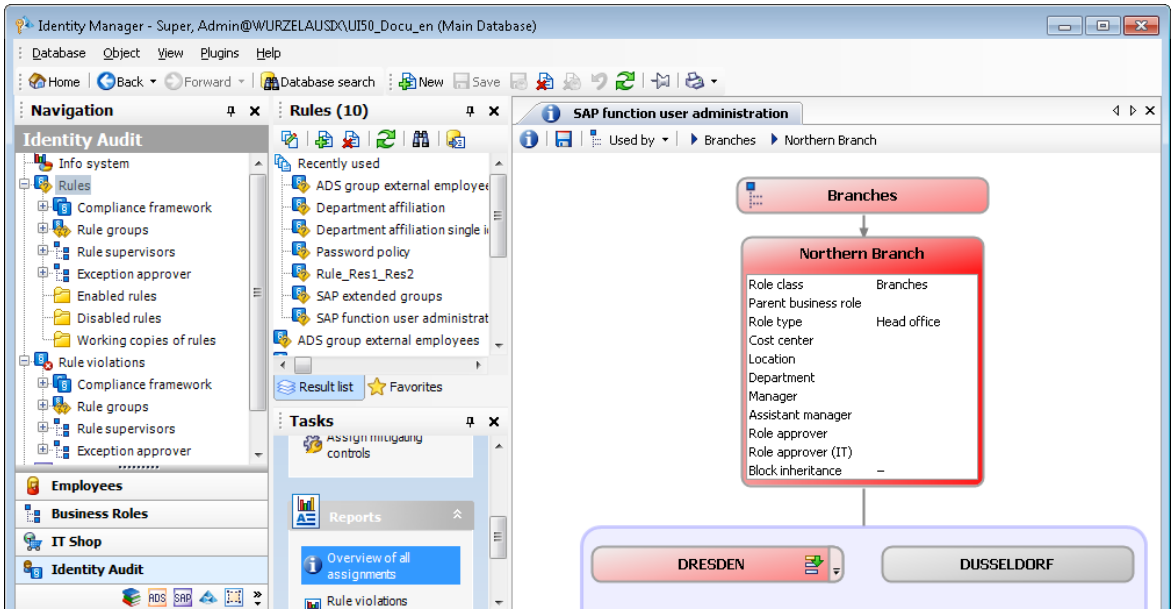
Reports about Rule Violations

The Identity Manager makes various reports available containing information about the selected base object and its relations to other Identity Manager database objects. The following reports are available for enabled rules with rule violations.

Overview of all Assignments

This report shows all employees that violate the rule in question. The report shows which roles of a role classe the employee belongs to. Employees that are not members of any role are not taken into account. What you get is an organigram of the different role classes for the selected rule.

Report "Overview of all Assignments" for a Compliance Rule



Use the <Used by> button in the report toolbar to select the role class for displaying the employee assignment you want to see. A simple mouse click on the control element in the report displays all the employees that violate the role and are members of the selected role. The meaning of the various control elements is described in section Overview of All Assignments on page 173 of the Getting Started Manual.

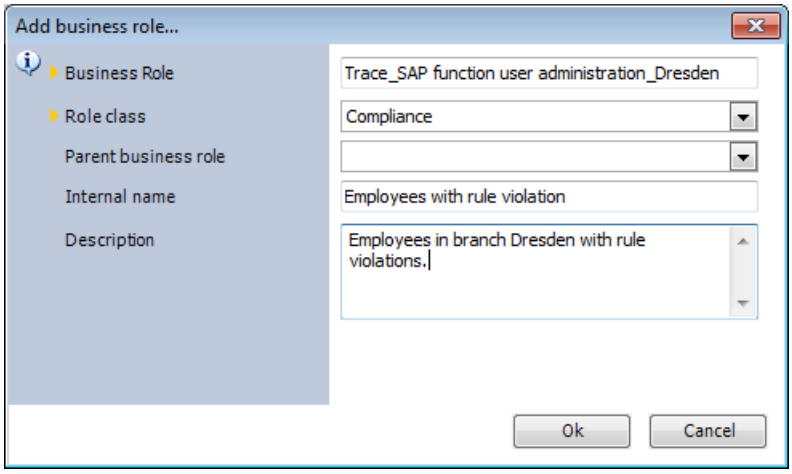
Use the small arrow on the right margin of the control element to start a wizard that allows you to bookmark this list of employee for tracking.

Bookmark Employee for Tracking

To do this a new business role is added and the employee are assigned to it.

The business role can only be added if you are logged onto the Manager.

Wizard for Tracking Employee Assignments



Enter the following data for the business role:

- Business role
  The name of the business role is made up automatically from the selected system entitlement and role. You can change the name as you wish.

- Role class
  Select a role class that is assigned to the business role. The drop-down menu shows all the custom defined role classes that can be used for the employee assignment.
  Role classes cannot be changed once they have been saved.

- Parent business role
  The new business role can be assigned to a existing business role as a child role.

- Internal name
  Additional internal name for the business role.

- Description
  Detailed description of the business role.

Use the <OK> button to save the business role and close the wizard. You are prompted by the Identity Manager to decide whether you want to display the business role straight away or not. If you confirm the prompt with the <Yes> button you can add more master data to the new business role. Close the prompt with the <No> button if you want to edit the business role at a later date.

Granting Exception Approval

Exception approval means that the employee no longer violates a rule. The employee is therefore not a member of the rule violation role anymore. Only employees that are assigned to the application role <exception approvers> can grant exceptions. The associated rule must have an exception approver assigned so that exception approvals can be granted for rule violations.

Use IT Shop to grant exception approval (see the Web Designer Manual). You can also grant exception approvals in the Manager. Proceed as follows:

Exception approval for all employees that violate a specific rule:

1. Select the category <Identity Audit>\<Rule violations>.

2. Select a rule violation and run the task <Show rule violations>.

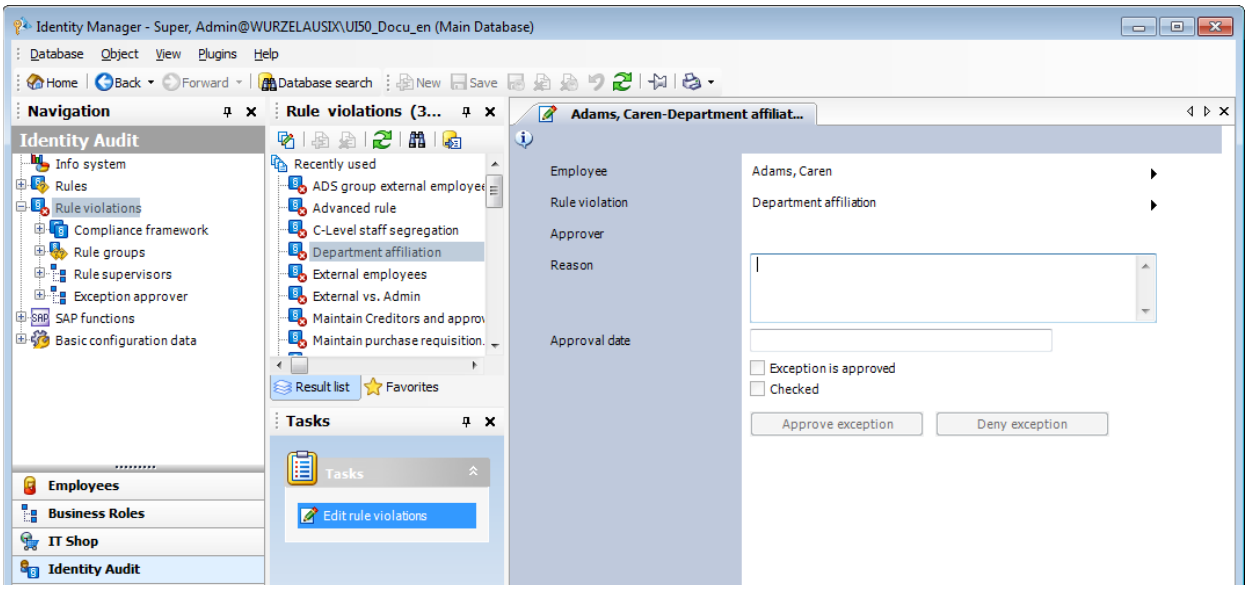
3. Select the employee that wants to be granted a rule exception (double click). The form <Rule violation: new> is opened.

4. A mouse click on the employee or the rule violation takes you to an overview form with information about the employee or therule violation.

5. Enter a reason.

6. Use the button <Approve exception> or <Deny exception> to make the decision about the rule violation.
   The fields <Approver> and <Approval date> as well as <Exception is approved> and <Checked> are filled out.

Exception Approval Form



Exception approval for all rules that violate a certain employee:

1. Select the category <employee>.

2. Select employee and view the report <Rule analysis>.

3. Select the rule violation for which you want to grant the employee exception approval (double mouse click). The form <rule violation: new> is opened.

4. A mouse click on the employee or the rule violation takes you to an overview form with information about the employee or therule violation.

5. Enter a reason

6. Use the button <Approve exception> or <Deny exception> to make the decision about the rule violation.
   The fields <Approver> and <Approval date> as well as <Exception is approved> and <Checked> are filled out.

Determining Potential Rule Violations

In addition to locating existing rule violation, the Identity Manager can also identify potential violations of IT Shop requests and business roles. This can clarify the following questions:

- Which rules might employees violate if this IT Shop request is approved?
- Which rules might an employee violate if they are added to this business role?

You can already identify possible rule violations by IT Shop requests within the approval procedure. Read more about this in the section Testing Requests for Rule Compliance on page 68 in the IT Shop Manual. Potential rule violation for business roles are displayed on respective overview forms. There are also reports available which show a detailed analysis of the violated rules and the assignments that lead to rule violations.

Identifying potential rule violations is done by analysis of the auxilary tables for object assignment. Prerequisite is, of course, that the auxilary table is regularly updated. For more information read the section Checking a Rule on page 449.

SAP Functions

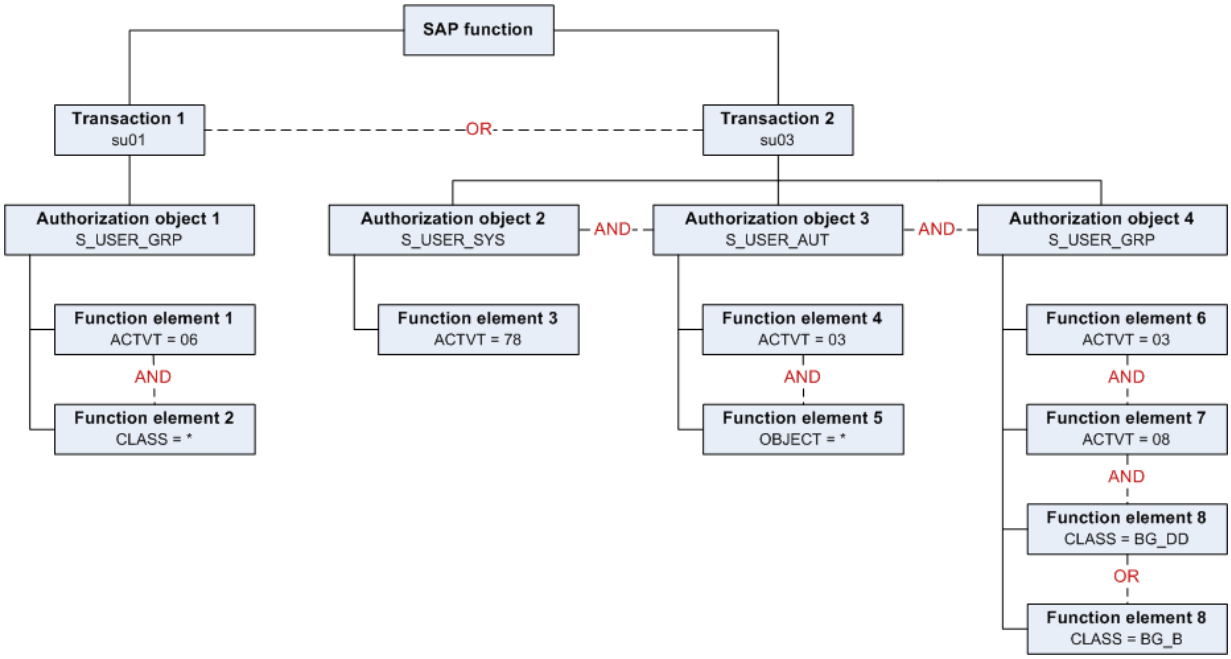
Apart from the rule checking options already described, the Identity Manager offers very detailed checking of effective user edit permissions for the target system SAP. By linking SAP users to employees, combinations of SAP authorizations that an employee obtains via different SAP users can be checked. Potentially dangerous SAP authorizations and combinations of them can easily be recognised this way and the neccessary action taken.

SAP authorizations are tested on the basis of permitted transactions for an SAP user and the associated authorization objects. To do this you have to define the transactions and authorization objects you want to check as SAP functions in the Identity Manager. Use compliance rules to check whether the SAP functions are permitted in this combination for an employee. An SAP role matches an SAP function if the SAP profile for this SAP role contains at least one of the transactions that are defined in the SAP function. To do this, the SAP profile must have all the authorization objects for this transaction. If a function element with a list of several instances is defined for an authorization object, the SAP profile matches the SAP function if it has at least one of these instances.

Example:

An SAP function is defined with the following transactions, authorization objects and function elements.

SAP Function Example



All SAP groups, SAP roles and SAP profiles that have the following authorizations are determined by the SAP function shown in the diagram:

- Transaction 1 with authorization object 1, function elements 1 AND 2

OR

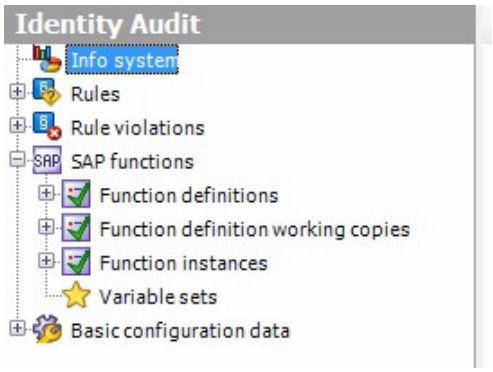
- Transaction 2 with authorization objects 2, 3 AND 4 and
  unction elements3, 4, 5, 6, 7 AND 8
  where function element 8 has the instance ”DOKU-BG-DD“ OR ”DOKU-BG-B“hat.

In order to check whether there are potenially dangerous SAP authorizations in the company, define SAP functions that are not permitted for these SAP authorizations. Find out which employees match these SAP functions by using compliance rules. Read the sections Setting up and Editing Rules on page 430 and Rule Conditions for SAP Functions on page 447 to find out how to set up compliance rules via SAP functions.

If employees are granted SAP authorizations via IT Shop requests, the SAP authorizations that are not permitted can be detected and handled respectively when the request is made with the appropriate approval procedures. For more information see section Testing Requests for Rule Compliance on page 68 in IT Shop Manual.

Define SAP functions in the Identity Manager in the category <Identity Audit>\<SAP functions>. To do this, log in with a role based authentication module from the application role <Identity Audit>\<Administrators>. You can also define SAP functions in the Manager.

SAP Functions



Prerequisites

Configuration Parameters for Handling SAP Functions

CONFIGURATION PARAMETERS	MEANING
TargetSystem\SAPR3\SAPRights	Preprocessor relevant configuration parameter to control modules for managing SAP autohorizations. After changes to this parameter the database must recompiled. If the parameter is enabled the target system modules are available.

In order to set up SAP functions, you need to set the configuration parameter TargetSystem\SAPR3\SAPRights and then compile the database. For more information see sections Compiling an Identity Manager Database on page 100 in the Getting Started Manual and Preprocessor Relevant Configuration Parameters on page 244 in the Configuration Manual.

All the information regarding SAP authorizations, users, roles and profiles must be transfered to the Identity Manager database so that Identity Manager can test the effective SAP authorizations based on SAP functions. To do this you synchronize the objects listed below. Depending on which synchronization method you use, enable the corresponding configuration parametes or configure the synchronization on the SAP client. You can find a more detailed description of each parameter in the Designer. See chapter System Configuration Parameters on page 214 in the Configuration Manual for more information.

Synchronization Objects Types and Assignments for SAP Functions

OBJECTS TYPES	CORRESPONDING CONFIGURATION PARAMETER
TRANSACTION	TargetSystem\SAPR3\SyncObjects\Transaction
TOBJC	TargetSystem\SAPR3\SyncObjects\TOBJC
TACT	TargetSystem\SAPR3\SyncObjects\TACT
AUTHX	TargetSystem\SAPR3\SyncObjects\AUTHX
USVART	TargetSystem\SAPR3\SyncObjects\USVART
TMENUE01	TargetSystem\SAPR3\SyncObjects\TMENUE01
TOBJ	TargetSystem\SAPR3\SyncObjects\TOBJ

Synchronization Objects Types and Assignments for SAP Functions

OBJECTS TYPES	CORRESPONDING CONFIGURATION PARAMETER
GROUP	TargetSystem\SAPR3\SyncObjects\Group
ROLE	TargetSystem\SAPR3\SyncObjects\Role
PROFILE	TargetSystem\SAPR3\SyncObjects\Profile
USER	TargetSystem\SAPR3\SyncObjects\User
AUTH	TargetSystem\SAPR3\SyncObjects\AUTH
SAPAUTHOBJECTOBJCT	TargetSystem\SAPR3\SyncObjects\SAPAUTHOBJECTOBJCT
SAPMENUEREF_OBJECT	TargetSystem\SAPR3\SyncObjects\SAPMENUEREF_OBJECT
SAPAUTHOBJECTFIELD	TargetSystem\SAPR3\SyncObjects\SAPAUTHOBJECTFIELD
SAPTRANSACTIONAUTHOBJECT	TargetSystem\SAPR3\SyncObjects\SAPTRANSACTIONAUTHOB-JECT
SAPGROUPAgr_Name	TargetSystem\SAPR3\SyncObjects\SAPGROUPAgr_Name
SAPGROUPAUTH	TargetSystem\SAPR3\SyncObjects\SAPGROUPAUTH

Base Data for SAP Functions

The following base data of relevant for SAP Functions:

- Mitigating controls
  Mitigating controls can be stored for SAP functions. These reduce the effects on the company when SAP users match with SAP functions. At the same time, you specify how to deal with SAP users that match with SAP functions. For example, changes to an SAP role user assignment in the SAP system can represent a suitable mitigating control for an SAP function. Read the section Setting up Mitigating Controls on page 428 for more information.

- Functional area
  In order to analyse the result of SAP function test for different role, set up a function area. Assign SAP functions to the functional area that are relevant for the analysis. The section Functional Areas on page 86 describes how to set up company area.

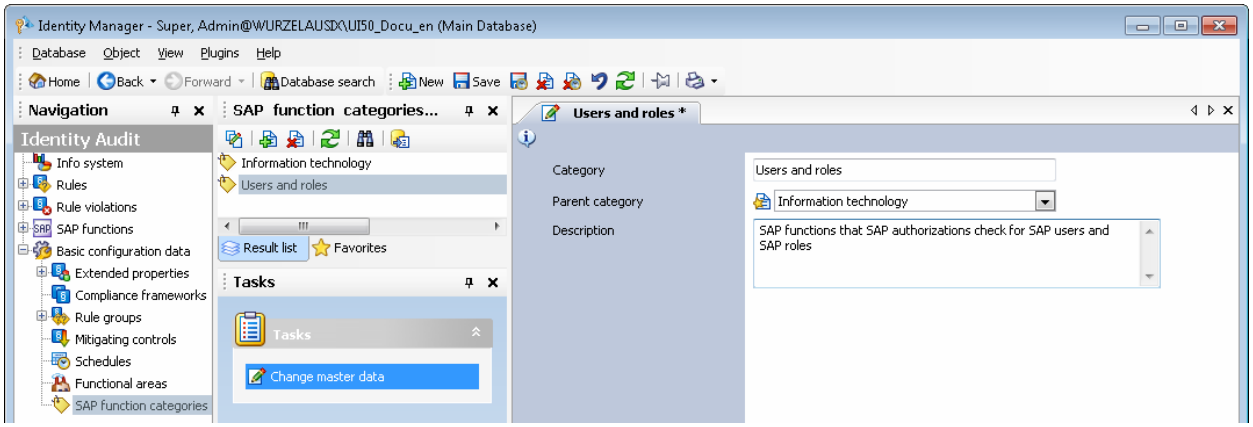
- SAP function categories
  Use SAP function categories to groups SAP functions under specific criteria. The section SAP Function Categories on page 460 describes how to set up function categories.

- Maintaining SAP functions
  An SAP function can be assigned to employees that manage the SAP functions and there for can edit the working copies. To do this, assign an application role <Maintain SAP functions> in the SAP function master data. Assign the employees that are authorized to enable and edit working copies of this SAP function and to define function instances to this application role. You can assign managers for SAP functions in the Manager in the category <Identity Audit>\<Basic configuration data>\<Maintain SAP functions> or in the Identity Manager in the category <Identity Manager Administration>\<Identity Audit>\<Maintain SAP functions>. See chapter General Master Data for an SAP Function on page 461 for more information about how to assign managers to SAP functions.

SAP Function Categories

Use SAP function categories to groups SAP functions under specific criteria. Enter SAP function categories in the category <Identity Audit>\<Basic configuration data>\<SAP function categories>.

Setting Up SAP Function Categories



Enter a unique name and a detailed decsription. Assign a parent category if you want to structure SAP function categories hierarchically.

Setting Up SAP Functions

Enter the general master data for an SAP function and the authorization definitions. An authorization definition consists of at one transaction. A least one authorization objects belongs to a transaction. Each authorization object consists of at least one function element (activity or authorization field) with concrete instances. Instances are given as single values or as upper and lower scope boundaries. Function elements can be listed more than once per authorization object.

SAP function are always edited using a working copy. The changes are not passed on to the SAP function until the working copy is enabled. SAP functions are displayed in the category <Identity Audit>\<SAP functions>\<Function definitions>; the working copies in the category <Identity Audit>\<SAP functions>\<Function definition working copies>.

Adding a New SAP Function

Add new SAP functions in the category <Identity Audit>\<SAP functions>\<Function definitions> using the <Creates new object> button. This, initially, creates a working copy. Once you have entered all the master data, enable the copy with the <Enable working copy> task. SAP authorization are only checked with respect to enabled SAP functions. The working copy is retained and can be used to make changes later.

Editing an Existing SAP function

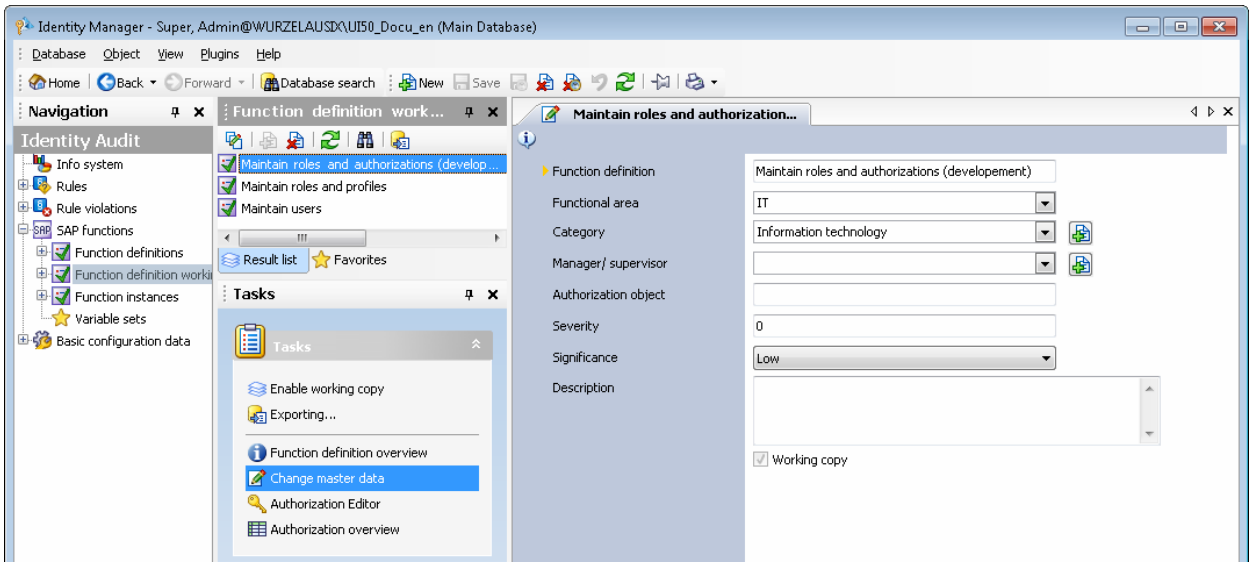
Existing SAP functions are edited in your working copy. To do this, run the task <Create working copy> for the function definition. The data from the existing working copy are overwritten with the data from the original after prompting. The working copy is opened and can be edited. After you have saved the working copy, transfer the changes by running the task <Enable working copy> for the SAP function.

The Identity Manager users with the application role <Identity Audit>\<Maintain SAP functions> can edit existing working copies that they are entered as being responsible for in the master data.

General Master Data for an SAP Function

Enter the master data for an SAP function on the master data form of the working copy. Ensure you full out all the mandatory fields..

General Master Data for an SAP Function



Enter the following master data for an SAP function:

- Function definition
  Unique ID for the SAP function.

- Functional area
  Functional area relevant to the SAP function.

- Category
  Assign an SAP function category if you want the SAP function to be grouped by a certain criterion. Use the button next to the input field to create a new function category (see section SAP Function Categories on page 460).

- Managers or Supervisors
  Select an application role, <Identity Audit>\<Maintain SAP functions> from the pop-up menu. All the employees that are assigned to this role are responsible for the context of this SAP function. Managers or supervisors can edit and enable working copies of the SAP functions assigned to them in the Identity Manager. Furthermore, they can define function instances and variable sets for these SAP functions.
  You can add new application roles for managers or supervisors via the button next to the input field. The procedure corresponds to that of adding and maintaining rule supervisors and exception approvers. Refer to section Maintaining the Rule Supervisor and Exception Approvers on page 432 for more information.

- Authorization objects
  Spare text field for entering information about the authorization objects that are used in the function definitions.

- Severity
  Specifies what it means to the company (or the assigned functional area) when an SAP user matches this SAP function. Enter a value from 0 to 1.

0 ... only information
1 ... Every SAP user that the SAP function matches, requires changes to the SAP authorizations that are effected.

- Significance
  Enter a verbal description of the effects on the company (or the functional area) when an SAP user matches this SAP function. The list of values { , low, medium, high, critical} are shown in the default installation.

- Description
  Detailed information about the SAP function.

- Working copy
  If this option is enabled, it means you are dealing with a working copy.

Additonal Tasks for Working Copies

The moment master data has been entered for an SAP function you can apply several tasks to the working copy. Use the overview form to get the most important information about the SAP function. In the task view you can select the tasks described below.

Authorization Editor

Use the Authorization Editor to set up the SAP function authorization definition. To do this, group transactions and authorization objects together that should be covered by the SAP function. The following tasks are available for this:

1. Add via menu template
   You can select menu items from the SAPGUI SAP menu (option <show SAP menus>) or from all the other SAP menu (option <All other menus>). Specify which SAP system should be used to display the menu tree. Select the menu items you want from the menu tree. All the transaction and authorization objects are loaded that can be called from the selected menu items.
   Transaction codes that are linked to a menu item are shown in brackets in the menu tree as additional information.

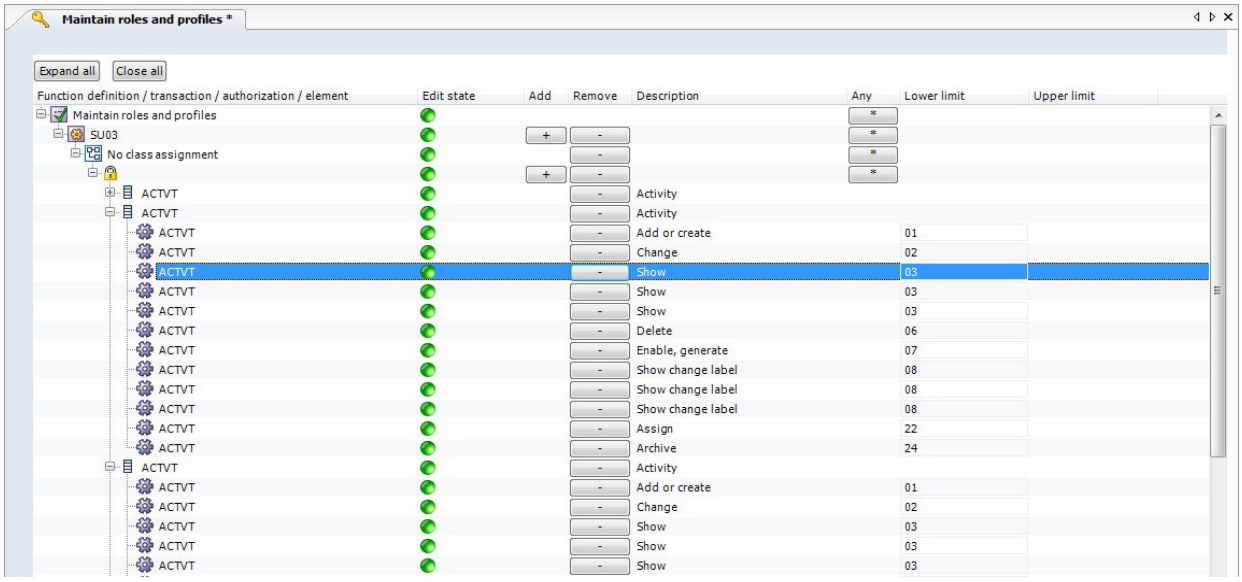
2. Add via transaction
   Select the transaction to load its authorization objects into the Authorization Editor. Use a filter to limit the transactions shown in the pop-up menu. All the authorization objects that are linked to the transaction are added.

3. Add via authorization object
   Select an authorization object to load into the Authorization Editor. Use a filter to limit the authorization objects shown in the pop-up menu. All transactions that the authorization object is linked to are added.

4. Add via existing function definition
   Select an existing function definition to loads its authorization definitions in the Authorization Editor.

When you have loaded the transactions and authorization objects you want into the Authorization Editor, specify the details for each function element. The functionality of the Authorization Editor is based on the SAPGUI Authorization Editor.

Authorization Editor for SAP Functions



The columns have the following meaning:

- Function definition/transaction/Authorization/element
  Transactions and their associated authorization objects and function elements are displayed in a tree structure under the function definition.

- Edit state
  An edit state is shown for each object in the tree structure.
  YELLOW ... There is no value defined for the function.
  GREEN ... Value is specified for the function element.

- Add
  Use this button to add more authorization definition objects.

- Remove
  Use this button to remove objects from the authorization definition.

- Description
  A description is shown in the menu for each object.

- Any
  Use this button to specify a wildcard value (”*“) for a function element.

- Lower limit and values
  Specify valid values for a function element here. For example, you can limit SAP authorizations to specific SAP groups. When you specify a range, enter the lower limit here. Values can be given as a variable using the notation ${alphanumeric}+$. Read the section Adding Vari-

able Sets on page 467 for more information about variables. Furthermore, you can also add system variables. The following notation applies to system variables, ${character}+.

Syntax of Values in Authorization Input Fields

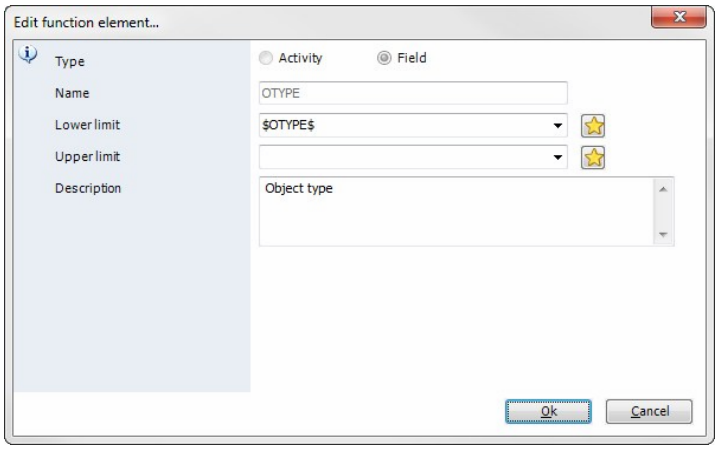
SYNTAX (EXAMPLE)	SAP AUTHORIZATIONS TESTED FOR	EXAMPLE OF INPUT VALUE IN SAP SYSTEM
*	any value	ab | 1234
Any character string (ab)	Exactly the given value	ab
[*]	the value *	*
Character string [*] (ab[*])	Values that start with the given string and end with *.	ab*
Character string* (ab*)	Values that start with the given string and end with any string	ab* | abcd
Comma delimited list (ab, 1234, c*)	One the values contained in the list	ab | 1234 | c* | cde
Variable (Var)	The value defined by the variable	
System variable ($Var)	The value defined by the system value	

- Upper limit
  When you specify a range for a function element, enter the upper limit here. Values can be given as variables in ther notation ”${alfa numeric}+$“. Read the section Adding Variable Sets on page 467 for more information about variables.

All function elements in a transaction that are defined in a separate row must be fulfilled for the SAP function to match. If the SAP functions should only match when an SAP profile has one of several possible instances of one and the same function element, define this instance as a comma delimited list of values for this function element.

Double-click on a function element to edit properties of the selected object.

Editing a Function Element



You can edit the description of the function element and the upper and lower limits.

- Type
  Specifies whether the selected function element is an activity or a authorization field.

- Name
  Unique name for the function element.

- Lower and upper limits
  You can select base values using the pop-up menu that are stored with the authorization field in the database (table SAPRCValue). Only the base value that marked as function template for this client are shown (see section General Master Data for a Client on page 352).
  You can select variables from variable definitions using the button next to the input fields.

- Description
  Detailed description of the function elements.

Check Authorization Objects for Completeness

The Identity Manager uses this task to test whether all authorization objects that belong to a transaction occur in the authorization definition. Missing authorization objects are displayed in a separate window. Enable the <Add> option on the authorization object you want to add to the authorization definition. Close the window using the <OK> button. The authorization objects can now be edited in the authorizations editor.

Authorization Overview

Function elements are disaplayed in a flat structure in the authorization overview. You can edit all the object properties here.

Enable Working Copy

SAP authorizations are only checked on the basis of active SAP functions. To make changes to a working copy in a function definition, run the task <Enable working copy>. For futher explanation see the section Setting Up SAP Functions on page 460.

Export...

Use this task to export authorization definitions to a CSV file. The SAP finction name and assigned function categories are exported as extended properties. The following properties are exported: function definition name, category, description, effect, transactions, authorization objects, authorization fields, description of authorization fields, value/lower scope boundary, upper scope boundary. An import status (”State‟) is included with each data record in the CSV file as additional information. The import status is set to ”1‟ by default on export. You can find more information about importing function definitions in section Import Function Definitions on page 469.

Addition Tasks for Function Definitions

Once a working copy is enabled you can apply several tasks to the function definition. You will find the most important information about the SAP function on the overview form. Furthermore, you can select the following tasks in the task view.

Create Mitigating Controls

Mitigating controls can be stored with SAP functions. These are used to limit the effects on the company when an SAP user matches the SAP function. At the same time, you specify how to deal with SAP users or SAP groups that match the SAP function. For example, changing a user assignment to an SAP role in the SAP system can be used as a mitigating control for an SAP function.

Mitigating controls can also be used as controlling measures for compliance rules. Properties for mitigating controls are described in the section Setting up Mitigating Controls on page 428.

Mitigating controls assigned to the SAP functions for testing are automatically transfered into compliance rules about SAP functions. Conditions:

- Active rules are assigned to a functional area and a department.
- The SAP functions for testing are assigned to the same functional area and then associated variable set of the same department.

Create a Working Copy

Apply the task <Creating working copy> to a function definition in order to modify an existing function definition. The data from the existing working copy is overwritten by the original SAP function data after prompting. For further explanation about this see section Setting Up SAP Functions on page 460.

Assign Mitigating Controls

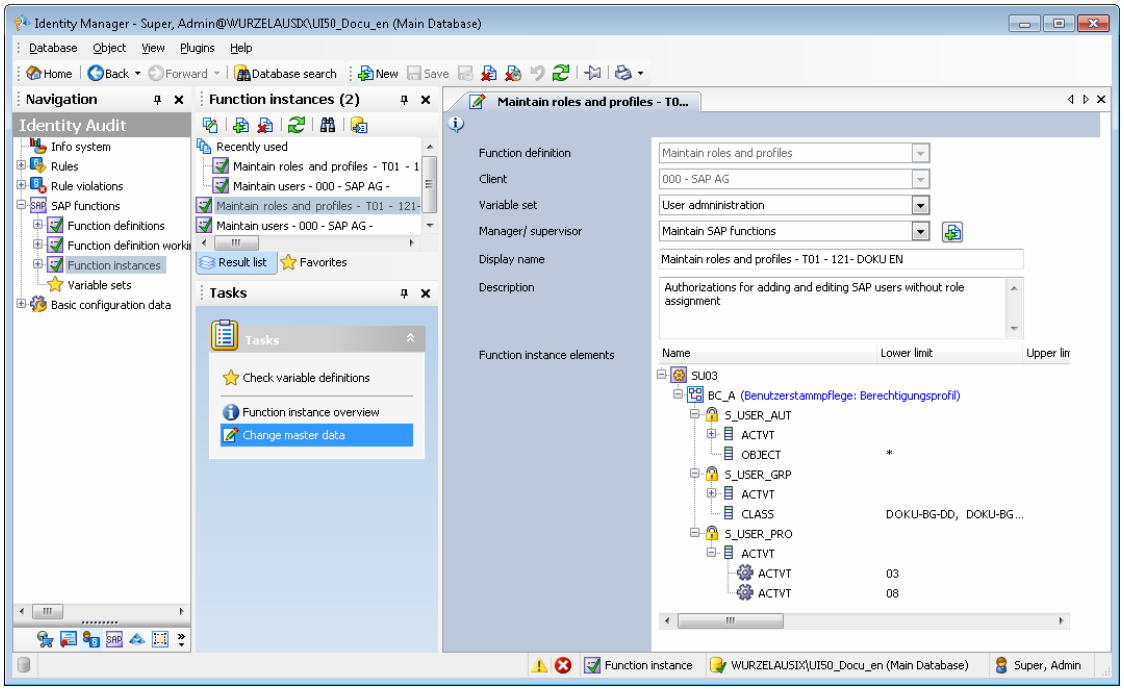
Use this task to specify which mitigating controls to apply for the selected SAP functions.

Define Function Instances

The Identity Manager provides the option of using the same function defintion for different specific instances. A specific SAP client that the SAP function will be used in, is given in the function instance. In addition, the variables that are assigned to the authorization fields are given speicifc values. Function instances can only be created for SAP functions that are enabled.

Edit function instances in the category <Identity Audit>\<SAP functions>\<Function instances>. To do this, log into the Identity Manager with a role based authentiation module from the application role <Identity Audit>\<Administrators>. The Identity Manager users can create and edit function instances for those SAP functions that they are responsible for..

Creating a Function Instance



Enter the following master data for a function instance:

- Function definition
  The function instance is created for this function definition.

- Client
  SAP client that the SAP function should be applied to.

- Variable set
  Assign a variable set which contains variables that are used in the function definition. Read section Adding Variable Sets on page 467 about creating variable sets.

- Manager/supervisor
  Select an application role, <Identity Audit>\<Maintain SAP functions>, from the pop-up menu. All employees that are assigned to this application role are responsible for the content of the function instance. You can also define a variable set.
  Add new manager application roles via the button next to the input field. The process corresponds to that for adding and maintaining rule supervisors and exception approvers. Read section Maintaining the Rule Supervisor and Exception Approvers on page 432 for more information.

- Display name
  This is formatted automatically fromthe function definition name, the assigned client and variable set.

- Description
  The description is taken from the function definition and be be extended.

- Function instance elements
  Displays transaction, approval objects and function elements for the SAP function with specified values that are determined from the variable set assigned. Changes to the variables or variable set are displayed as soon as the DB Scheduler has processed the corresponding authorization tasks.

Additional Tasks for Function Instances

As soon as a function instance has been created you can apply different tasks to it. You will find the most important information about the function instance on the overview form. Furthermore, you can select the following tasks in the task view.

Check Variable Definitions

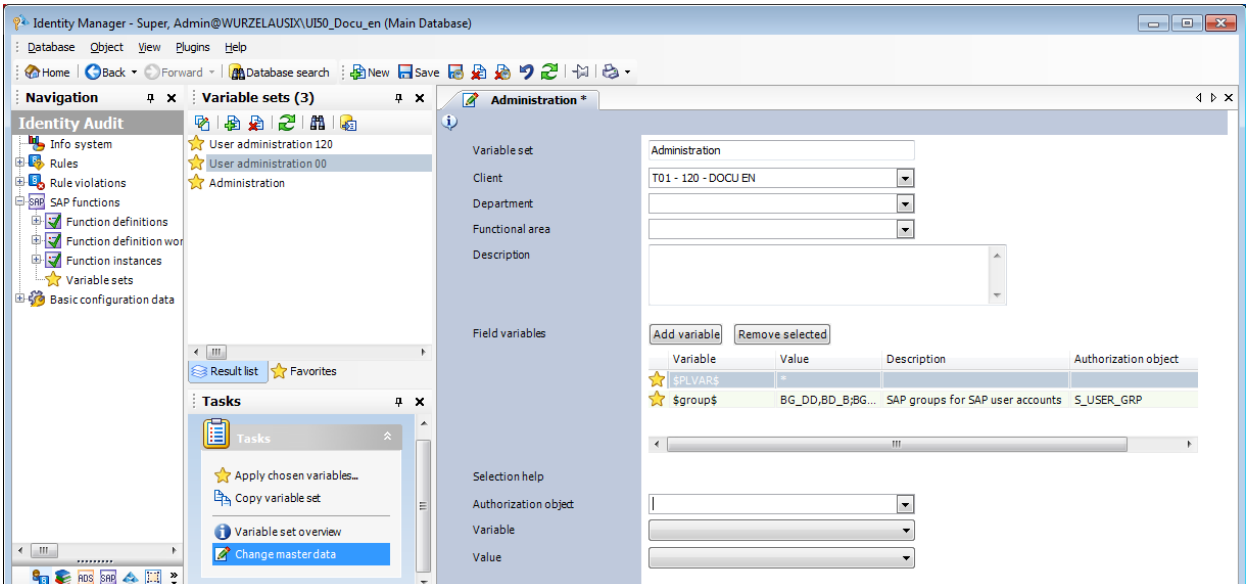
The Identity Manager checks whether all the variables to be used in the function definition are defined in the assigned variable set. If there is no function definition or variable set assigned to the function instance, the check is fails with an error message. Variables that are not defined in the associated variable set are listed in the error message.

Adding Variable Sets

Use variable sets to group variables together that are used in an authorization definition and give then fixed values. Edit variable sets in the category <Identity Audit>\<SAP functions>\<Variable sets>. To

do this, log in with a role based authentication module from the application role <Identity Audit>\<Administrators> or <Identity Audit>\<Maintain SAP functions>..

Creating Variable Sets



Enter the following master data for variable sets:

- Variable set
  Unique variable set name

- Client
  Valid SAP client for the variable set.

- Department
  Relevant department for the variable set.

- Functional area
  Relevant functional area for the variable set.

- Description
  Detailed description of the variable set.

- Field variables
  List of defined field variables.
  Use the <Add> button to enter a new line in the list. Enter the variable a name in the notation ”${alphanum}+$“. Enter the fixed instance for the variable in the <Value> column that will be transferred to the function instance. Give the variable a description. In the <Authorization object> column, you can link to the authorization object that the variable should be used in.
  Use the <Remove selected> to delete the variables marked in the list.

Variable names may not start with system variable names. This can lead to error. Variable sets with variables of this type cannot be saved.

On the form, there is help available for selecting SAP system authorization fields and organizational levels for an authorization object to be used for defining variables. If SAP system basic values are stored with an authorization field, these are provided in the pop-up menu <Value>.

You can add variable sets without defining variables.
Use these variables set for function definitions that do not have variables entered as values.

Additional Tasks for Variable Sets

As soon as a variable set has been created you can apply different tasks to it. You will find the most important information about the variable sets on the overview form. Furthermore, you can select the following tasks in the task view.

Apply Chosen Variables...

Variables that are used in SAP functions are transfered to the variable set using this task. To do this, mark the function definitions or working copies that you want to copy the variables from in the dialog window Multi-select is possible.

Copy Variable Set

Use this task to create a copy of the select variable set. Then you can edit the master data in the copy.

Plugins for SAP Functions

There are two plugins available for SAP functions. Run the plugins from the menu <Plugins> in the menu bar. You can use the plugins to swap SAP functions between the Identity Manager databases.

Export Function Definitions

Use the menu item <Export all SAP function definitions...> to write all existing SAP functions to a CSV file. Specify whether only a working copies or only enabled SAP functions should be exported. All function definitions are written to file in sequence. The following properties are exported: function deinition name, category, description, effect, transaction, Authorization objects, authorization fields, description of authorization fields, progresss state, value/lower scope boundary, upper scope boundary. An import status (”State“) is included with each data record in the CSV file as additional information. The import status is set to ”1“ by default on export. This data is evaluated when function definitions are imported.

Import Function Definitions

If you want to import SAP functions from an existing CSV file, use the plugin >Import SAP functions...>. The functions definitions contained in the CSV file are transfered to the database as working

copies. If there is already a working copy with the same name in the database, it is overwritten by the import. The following data fields must be in the CSV file so that function definitions can be imported.

Data Fields for Importing Function Definitions

DATA FIELDS IN THE CSV FILE (HEADER)	OBJECT PROPERTIES IN THE IDENTITY MANAGER
Mandatory fields:	
Function	Function definition
Transaction	Transaction
Object	Authorization objects
Field	Authorization field
Value From	Value/lower scope boundary
Value To	Upper scope boundary
State	No equivalent The import status controls which data records are imported into the Identity Manager. 1 ... import
Optional fields:	
Process	Categorie
Function Description	Description of the function definition
Risk Level	Effect Possible values are {Low|Medium|High|Critical}.
Field Description	Describes the authorization fields, authorization objects and transactions

14

Attestation and Recertification

- Introduction
- Defining Attestation Instances
- Monitoring Attestation Instances

Introduction

Attestation is characterized by data, internal rules and controls for authorization. Managers or others responsible for compliance can use the Identity Manager attestation function to certify access permissions, authorizations, requests and exception approvals. ”Recertification“ is the term generally used to described regular certification of permissions. The Identity Manager uses the same workflows for recertification and attestation. Recertification is therefore treated as a special case of attestation in the Identity Manager. In the following, we will use the word ”attestation“ to cover both terms.

In order to run attestations automatically and on a regular basis you can define different attesation policies. You use these policies to specify, which objects are designated for attestation, who performs the attestation, when and how frequently the attesations should be carried out. When an attestation is performed, the Identity Manager creates a report for the attestor responsible. The attestor checks the report. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules. Attestation is rerun once the changes have been made.

Defining Attestation Instances

General Configuration Parameter for Attestation

CONFIGURATION PARAMETER	MEANING
QER\Attestation	Preprocessor relevant configuration parameter for controlling the model parts for attestation. After changes have been made the database has to be compiled. If the parameter is enabled you can use the attestation function.

Define attestation instances in the Identity Manager in the category <Attestation>. You need to log in with a role based authentication module included in the <Attesation>\<Administrators> role.

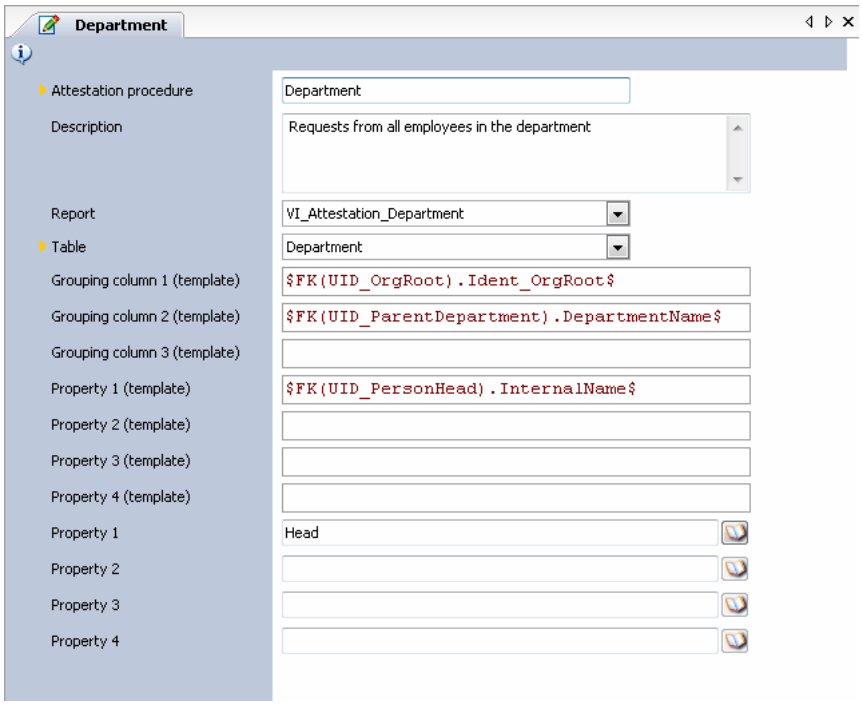
Entering Base Data

Enter attestation base data in the category <Attestation> in the filter <Basic configuration data>. Here you can specify attestation procedures, schedules and approval policies.

Attestation Procedures

For each attestation procedure, enter a name and the objects to be subject to attestation. You can also define a report form to contain information for the attestor about the objects.

Master Data Entry for Attestation Procedures



Enter the following data:

- Attestation procedure
  Arbitary name for the attestation procedure.

- Description
  Addition information about the attestation procedure.

- Report
  Report for the attestor containing all the necessary information about the attestation objects. Predefined reports are supplied in the input field's drop-down menu. If you do not assign a report, the attestation instances are listed without extra information in the IT Shop.

- Table
  The database table to take the attestation objects from (= attestation base object).

- Grouping columns 1-3 (template)
  A value template for formating the value used to group pending attestation instances in IT Shop.
  Enter a value template in $ notation. As soon as you enter ‚$' into the input field, a drop-down menu is displayed. Select the database column whose values form the basis for the grouping criterion. The template syntax is described in section Using $ Notation on page 321 of the Configuration manual.

- Property 1-4 (template)
  Templates for formulating a value that forms the basis for sorting pending attestation instances in the IT Shop. Use these fields to show additional information about the attestation object in the attestation instance.
  Enter a value template in $ notation. As soon as you enter ‚$‘ into the input field, a drop-down menu is displayed. Select the database column whose values form the basis for the grouping criterion. If you select an FK column, you can navigate to the columns of the associated table using the cursor keys. Finalize you selection with the enter key or double-click with the mouse.The complete $ notation for your selection should now be shown in the input column.The template syntax is explained in the section Using $ Notation on page 321 in the Configuration Manual.

- Property 1-4
  Here you can specify column headings for the sort column property 1-4 (template). Use the button next to the input field to translate the entries. You can find more detailed information about translating multilanguage columns in the Configuration Manual in section Language Dependent Input in Administration Tools on page 201.

Example:

The attestation objects should be from all departments that are entered in the Identity Manager. Attestation instances should be grouped by base object and beneath that by parent department. The information required about the attestation objects should be summaried in a report. To do this, enter the following data on the master data form.

Table: database table ”Department“
Report: <report name>
Grouping column 1: $FK(UID_OrgRoot).Ident_OrgRoot$
Grouping column 2: $FK(UID_ParentDepartment).DepartmentName$

The relation to base object and to the parent department is formed in the database table ”Department“ through the foreign key columns UID_OrgRoot and UID_ParentDepartment. The associated ”Ident_OrgRoot“ in the ”OrgRoot“ table must be selected along with the FK UID_OrgRoot so that the name of the base object is displayed as the first grouping criterion. This is achieved by the template in the grouping column 1. The name of the parent department is selected from the column ”DepartmentName“ of table ”Department“ in the same way. A report in PDF format is supplied for every attestation instance.

Defining Reports for Attestation

Define attestation reports with the Report Editor. The section Creating and Editing Reports on page 369 in the Configuration manual describes how to use the Report Editor.

The base tables for the report must be identical to the one for the attesation procedure. Enter ”Attestation“ to label the report. This ensures that the report is displayed in the menu for the attestation procedure <Report> data field.

Define a parameter ObjectKeyBase for the attestation object so that exactly the information for the affected attestation object is reported for each attestation object. Include the parameter in the definition of the data source for the report.

```
where <Tabelle>.XObjectKey = @ObjectKeyBase.
```

Schedules

Schedules are used to automate attestation. With schedules, you can specify when and how often attestation reports should be generated. Schedules are also used in the Identity Manager to test dynamic roles or compliance rules. The section Setting Up a Scheduled Task to Calculate Dynamic Roles on page 103 provides complementary information on how to set up schedules.

Assign schedules to attestation policies on the attestation policy master data form. This makes them available for attestation.

Additional Tasks for Schedules: Assigning Attestation Policies

Once you have entered the schedule master data, you may run the task <Assign attestation policies> from the task view. This task provides you with an overview of all the attestation policies that are assigned to the schedule.

Use the context menu item <Show objects already assigned to other objects> to display attestation policies that are already assigned to other schedules. If you double click on one of the attestation policies you assign it to the current schedule.

Do not remove any assignments! Attestation policies must be assigned a schedule, it is compulsory.
If you remove assignments and save the changes, you will get an error message. The changes cannot be saved.

Attestation Approval Policies and Workflows

The Identity Manager uses approval policies to determine the attestor for each attestation instance. Approval policies are used in the Identity Manager for making requests in the IT Shop. Approval policies are also used for request procedures in IT Shop. When you assign approval workflows to approval policies, you specify whether they are only used for attestation, only for IT Shop requests or for both.

You need to allocate an approval workflow to an attestation approval policy in order to find the attestors. Renewal and cancellation workflows are only relevant for attestation.

In an approval workflow, you specify the approval procedure, the number of approvers and a condition for selecting them if necessary. Use the Method Editor to create and edit approval policies. How to use the Method Editor is described in full in the section Approval Processes for IT Shop Requests on page 52 of the IT Shop manual.

Attestation Approval Procedures

Approval procedures determine the approver (=attestor) for the actual attestation procedure. Whether an approval policy can only be used for attestation or IT Shop requests or both depends on the approval procedure. The Identity Manager provides the following approval procedures for attestation.

Approval Procedures for Attestation

ABBR.	PROCEDURE NAME	ATTESTOR
AD	Attestor for recipient's department	Attestor of the department that the attestation object is primarily assigned to. Employee with the application role <Attestor>
AL	Attestor for recipient's location	Attestor of the location that the attestation object is primarily assigned to. Employee with the application role <Attestor>
AO	Attestor for recipient's primary role	Attestor of the business role that the attestation object is primarily assigned to. Employee with the application role <Attestor>

Approval Procedures for Attestation

ABBR.	PROCEDURE NAME	ATTESTOR
AP	Attestor for recipient's cost center	Attestor of the cost center that the attestation object is primarily assigned to. Employee with the application role <Attestor>
AR	Attestor for attestation compliance rule	Asstestor for the compliance rul to be attested. Employee with the application role <Attestor>
AT	Attestor for attestation organization	Attestor of the organization that the attestation object is primarily assigned to. Employee with the application role <Attestor>
CD	Calculated approval	System Identity Manager, if the condition is met.
CM	Recipients Manager	Manager of the employee to be attested. Independent of the application role <Attestor>.
CP	Calculated group of approvers	Employees determined via a condition. Not dependent on the application role <Attestor>.
EX	Approvals to be made externally	System Identity Manager, if an external system triggers a defined process.
OR	Members of a certain role	All employees that are assigned to a secondary business role.
WC	Waiting for further approval	System Identity Manager, if a defined data state occurs in the Identity Manager database.

The approval procedures CD, CM, CP, EX, OR and WC can also be used for IT Shop requests.

AD, AL, AO, AP: Determining the Attestor using the Role of an Employee Marked for Attestation

When you want to attest company resource assignments to employees or your staff's requests, use the approval procedures AD, AL, AO or AP. The attestors that are found are members of the application role <Attestor>.

Attestation object are employees (table: Person) or requesters (table: PersonWantsOrg). AD, AL, AO and AP determine the role (department, location, business role, cost center) for each attestation object that the attestation object is primarily assigned to.

AR, AT: Determining Attestors using Attestation Objects

When you want to attest compliance rules or company resource assignments to departments, location or business roles, use the approval procedures A or AT. The procedure AT is also suitable for attesting assignments to IT Shop structures (shops, shopping centers or shelves). The attestors that are found are members of the application role <Attestor>.

Attestation objects for AR are compliance rules (table: ComplianceRule). Attestation objects are roles (tables: department, ITShopOrg, Locality, Org, ProfitCenter, ITShopSrc). A and AT determine the attestors that the attestation object is assigned to. If the attestation object is not directly assigned an attestor, the approval procedure finds the attestor from the parent node. If no attestor is found in this way, the attestation procedure for the attestor of the associated role class is passed on for approval.

CD: Calculated Approval

If you want to make attestation dependent on specific conditions, use the approval procedure CD. This procedure does not determine an attestor. The Identity Manager make the decision depending on the condition that is formulated in the approval step.

You can use the procedure for any attestation objects. You create a condition in the approval step. If the condition returns a result, the approval step is approved by the Identity Manager. If the condition does not return a result, the approval step is denied. If there are no further approval steps, the approval procedure is either finally granted or denied. The condition is defined as a database query WHERE clause. You can either enter it in SQL directly or by using a wizard. If you use the wizard, specify first specify whether the condition should be used for IT Shop or attestation. Refer to the condition via the variable @UID_AttestationCase in the definite case of an attestation instance.

Example of a simple approval workflow with the approval procedure CD:

Compliance should be tested when they meet the following conditions:
1. Compliance rule is enabled
2. A rule manager is assigned to the compliance rule.

Find the objects that meet these conditions by using the approval procedure CD.

```
EXISTS ( SELECT 1 FROM  (SELECT xobjectkey FROM ComplianceRule
WHERE isnull(IsWorkingCopy, 0) = 0
AND  EXISTS ( SELECT 1 FROM
 (SELECT UID_AERole FROM AERole WHERE 1 = 1)
 as X  WHERE X.UID_AERole = ComplianceRule.UID_OrgResponsible))
as X  WHERE X.xobjectkey = AttestationCase.ObjectKeyBase  )
```

If the condition is met, the rule attestor should attest this compliance rule. To do this, extend the positive approval path with an approval step using approval procedure AR.
If the condition is not met, the attestation should be denied by the Identity Manager. In this case, no further approval steps are required.

CM: Determining a Manager as Attestation Object Attestor

When you want to allow company resource assignments for your employee via their managers, use the approval procedure CM. Attestation objects are employees (table: Person). CM finds the manager associated with every attestation object that the attestation object is primarily assigned too.

CP: Dynamically Calculated Group of Approvers

Use the approval procedure CP if objects are to be attested by employees that are not members of the application role <Attestor>. You can allow any objects to be attested by any employees using this procedure. You set up your own database query that should find the attestor. The result of this query must by employees. Therefore a ”UID_Person“ column has to be found via the database query.

Example:

All active compliance rules should be attested by the respective rule supervisor. Use the CP procedure and the following condition to find the rule supervisor for each active rule.

```
select pia.UID_Person
from PersonInAERole pia
join ComplianceRule cr on pia.UID_AERole = cr.UID_OrgResponsible
join AttestationCase ac on ac.ObjectKeyBase = cr.XObjectKey
and ac.UID_AttestationCase = '@UID_AttestationCase'
where cr.IsWorkingCopy = '0'
```

EX: Attestation when an External Event Occurs

Use the approval procedure EX when attestation should take place the moment a event external to the Identity Manager occurs. You can also use this procedure to allow any number of objects to be attested by employees that do not have access to the Identity Manager.

Specify the event in the approval step that triggers the external approval decision. A process is started by the event that initiates the external approval for the attestation instance and evaluates the result of the approval decision. The Identity Manager waits until the result of the external decision is transmitted to the it. You define subsequent approval steps depending on this result.

In order to use the approval procedure EX, you define your own processes. These processes must trigger an external approval decision, evaluate the results of the external approval and based on this, start the subsequent approval steps in the Identity Manager. Enter ”AttestationCase“ as root object for the process. If the external has occurred the approval step status has to be changed. Use the process task ”CallMethod“ with the method ”MakeDecision“ for this. Only the system user ”sa“ can make these changes. In the process definition, pass the system user ”sa“ as parameter to the process task. You use the Process Editor to define and edit processes. How to use the Process Editor, is descibed in section Handling Processes in Identity Manager on page 37 in the Process Orchestration Manual.

Example:

All compliance rules should be checked and attested by an external assessor. The attestation object data should be made available as PDF on an external share. The assessor should save the result of the attestation in a text file on the external share. Use the approval procedure ”EX“ and define:

- A process <P1> that saves a PDF report with data about the attestation object data and the attestation procedure on an external share
- An event <E1> that starts the process <P1>
- A process <P2> that checks the share for new text files, evaluate the contents and calls the Identity Manager task ”Call method“ with the method ”MakeDecision“
- An event <E2> that starts the process >P2>
- A schedule that triggers the event <E2> on a regular basis.

Enter the event <E1> in the approval step in the input field <Event> as trigger for the external decision.

OR: Determining the Manager using Business Role Members

Use the approval procedure OR if objects are to be attested by employees or members of certain business roles. You can allow any objects to be attested by employees from any business role with this procedure. Specify a business role in the approval step. OR finds all employee that are members of the given business role via secondary assignment.

WC: Deferred Request Approval

If you want to ensure that a specific data state exists in the Identity Manager before attestation, then user the approval procedure WC. Use a condition to specify which prerequisites have to be fulfilled so that attestation can take place. The condition is evaluated as a function call. The function has to accept the attestation instance UID as a parameter (AttestationCase.UID_AttestationCase). Use this UID to refer to each attestation object. The result must be an integer value.

Function call in a deferred approval condition:

```
dbo.vi_F_PWOGroupDecision
```

One the following actions is carried out depending on the function‘s return value.

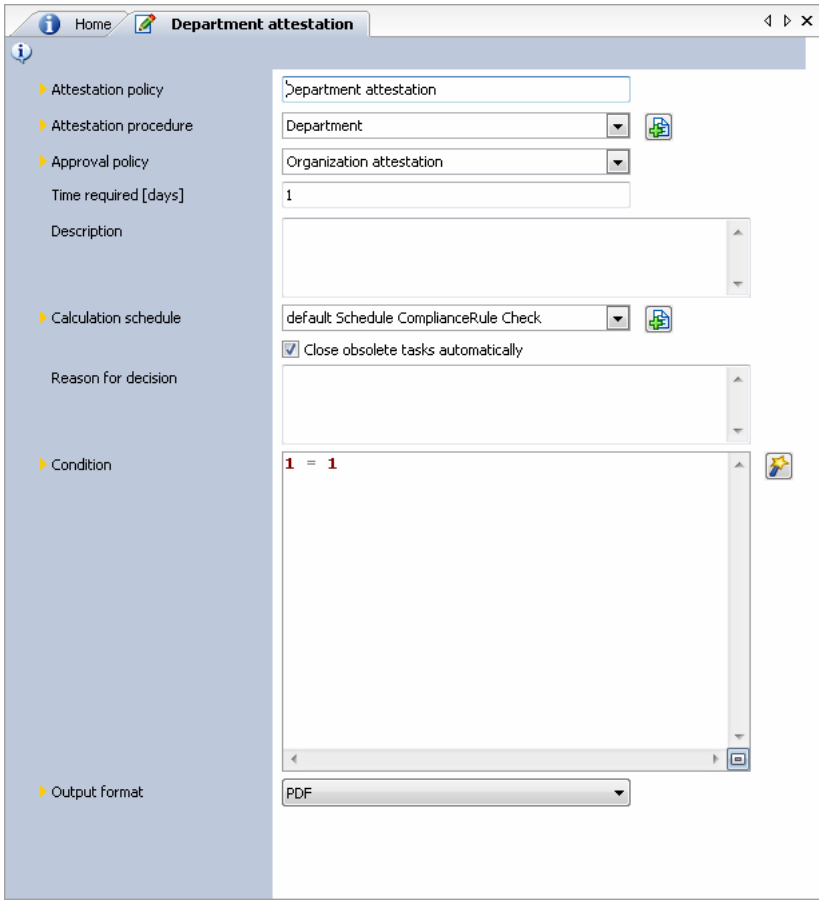
- Return value > 0: The condition is met. Deferred approval has completed successfully. The next approval step (in case of success) is carried out.
- Return value = 0: The condition is not met.The approval decision is postponed and retested again the next time the DBScheduler runs.
- Return value < 0: The condition is not met. Deferred approval has failed. The next approval step (in case of failure) is carried out.

If successful, specify an approval procedure in the pproval step that the Identity Manager can used to determine the attestators.

Setting Up Attestation Policies

Attestation policies specify the concrete conditions for attestation. Use the master data form to enter the attestation procedure, approval policy and the schedule. You can use a WHERE clause to limit the attestation objects.

Entering Master Data for Attestation Policies



Enter the following data:

- Attestation policy
  Any name for the attestation policy.

- Attestation procedure
  The name of the attestation procedure to be used for attestation.

- Approval policy
  The approval policy for determining the attestor for the attestation objects. Only those approval policies that are valid for attestation are displayed in the drop-down menu.

- Time required [days]
  The number of days required for the attestation approval. Enter ”0“ if you do not want to be specific.

- Description
  Additional informatio about the attestation policy.

- Calculation schedule
  Scheduled times for running the attestation. Attestation instances are started automatically at the times specified by the schedule.

- Close obsolete tasks automatically
  If the Identity Manager creates starts new attestation instances it checks whether unprocessed attestation instances from the same attestation policy and with the same attestation procedure still exist. These attestation instances are closed automatically.

- Reason for decision
  If the check box ”Close obsolete tasks automatically“ is set and unprocessed attestation instances are automatically closed, this is the reason that will be given.

- Condition
  The Identity Manager uses this condition to determine the attestation objects from the database table specified in the attestation procedure. Enter the condition as a valid WHERE clause for database queries. You can enter this directly as SQL query or use a wizard. Click the button next to the input field to start the wizard.

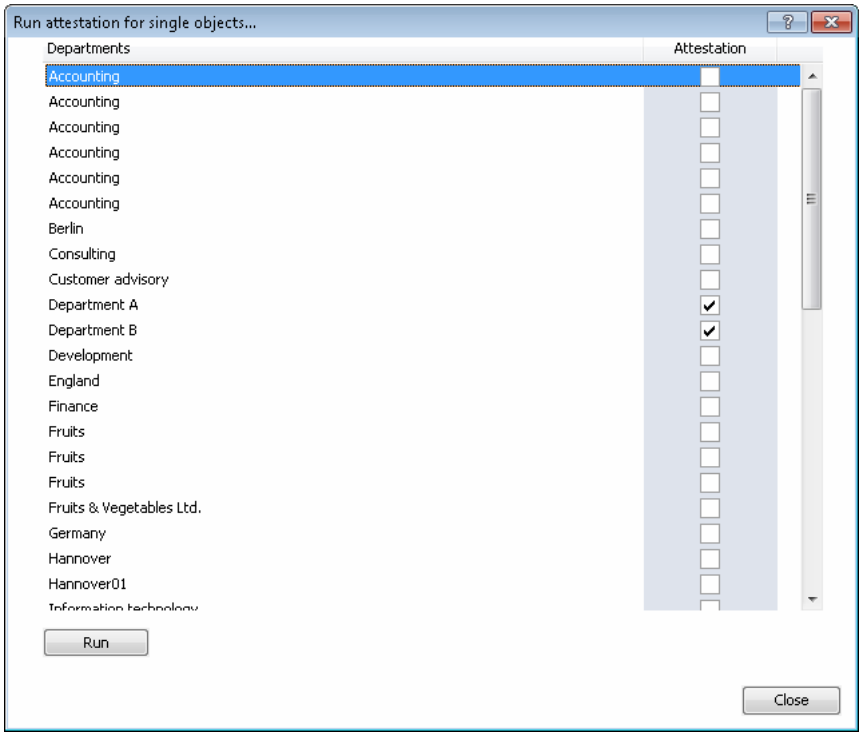
Additional Tasks for Attestation Policies

Once you have entered the attestation policy master data, you can apply various tasks to the attestation polices. The overview form supplies you with the most important information about an attestation policy. Furthermore, you can select the tasks described in the following in the task view.

Run Attestation for Single Objects

Use this task to start attestions independently from a schedule. If you run the task, a separate window is opened. Select the object that should attested from a list of all attestation objects. The selection is one-off.

Selection Window: Attestation for Single Objects



When you click the <Start> button, the attestation instances for the selected attestation object are initiated. Use the <Close> button to close the selection window. Once the DBScheduler has processed the request, you can view them in the navigation view under the menu item <Attestation instances>/<attestation policy name>/<Pending attestations>.

Monitoring Attestation Instances

Once attestation is automatically or manually started, the Identity Manager creates an attestation instance for each attestation object. You can view the attestation instances in the navigation view under the menu item <Attestation instances>/<name of attestation policy>. This is where you can monitor the status of the attestation instances.

Attestation instances that were not yet subject to approval are grouped under <Pending attestations>. You can see the attestation instances that have been processed by an attestor or have been closed by the Identity Manager grouped under <Closed attestations>. You can apply several tasks to the attestation instances.

Additional tasks for Attestation Instances

Attestation Instance Overview

The overview form provides you with the most important information about attestation instances. Apart from the processing time you can also see the time at which the the attestation instance should be completed. The Identity Manager does not supply the action to be carried out if the processing time is exceeded. You define company specific actions or analyses for this case.

Approval Sequence

The approval sequence is show as soon as an attestor is determined for the attestation instance. You can view the approval sequence and the attestor that has been found in the approval workflow. If the approval procedure could not find an attestor, the attestation instance is closed by the system. You cannot see the attestation sequence for this attestation instance.

The task <Approval sequence> can only be applied to open attestations.

Attestation History

The report ”Attestation history“ report displays individual steps of the attestation instance. Here you can follow the time taken and the approval decision for the attestation instance. The history is displayed for open as well as for closed attestations.

If you have selected a report in the attestation procedure, a report is created in PDF format for each attestation instance.

GLOSSARY

A

ABAP

Advanced Business Application Programming. Programming language from the company SAP AG.

Active Directory (AD)

LDAP based directory server from Microsoft that was introduced with Window 2000.

Active Directory Service

Directory service implementation from Microsoft.

Application

User software.

Application group

A global group for assigning applications to user accounts.

Application Link Enabling (ALE)

SAP technology for integrating and running distributed applications on different SAP systems.
Refer to your SAP sytem documentation for further details.

Application role

Identity Manager application roles are funtional roles that you use to specify entitlements to Identity Manager functions which result from Identity Manager user tasks from within the company structures. Application roles take administration and approval processes into account.
Application roles are preset but may be changed and extended.

Approval procedure

Method for granting approval for customer requests withing the IT Shop. An approval procedure is made up of approval policies that can contain several approval levels. Several approval steps can be defined for each approval level. A different approver can be specified for each approval step.

Approver

The approver is an employee that can grant or deny approval in a procedure for approving a request (renewal or cancellation).

Approval policy

Specifies which approval workflow should be in used IT Shop for an attestation instance or a request (renewal or cancellation).

Approval procedure

Finds the attestor for the current attestation instance or the approver for the current request (renewal or cancellation) in IT Shop.

Approval workflow

Specifies which approval procedure will be used in which order in attestation instances or requests (renewals or cancellations) in IT Shop. An approval workflow contains at least one approval level with at least on approval step.

Assignment request

Requests for company resources, employees for roles.
You can request assignments for departments, cost centers, locations or business roles via the IT Shop, then they are authorized via approval process.

Attestation

A method for authorizing data or internal rules.
Attestation functionality in Identity Manager is used by manager or other in authority to certify the correctness of editing permissions, entitlements, requests or exception approvals on a regular or manual basis.

Attestation instance

Objects that are created as soon as attestation is automatically or manually started.
When attestation is triggered, Identity Manager creates an attestation instance for each attestation object. Attestation data is saved in the attestation instance. This includes the attestation object, status (open, approved, denied), date of attestation, the attestor.

Attestor

The person that will carry out the attestation.
Attestors approve data that is presented in an attestation instance, or they deny it.

Authentication module

Authentication modules are used to define how user should log onto Identity Manager tools. Users can log in as, for example employees with their Active Directory user account or directly as system users. The authentication module determines which system user is directly or indirectly assigned to the logged in user. This assigns user permissions for the user interface elements of the administration tool that has been started and for the database objects.

Authorization definition

Group of transactions and authorization objects in Identity Manager to be tested by an SAP function.

Authorization Editor

Tool for edition the authorization definition for an SAP function.

Authorization Field

An object in an SAP system. The smallest unit that can be granted authorizations. To do this, authorization fields are given fixed values (activities of data). Up to 10 authorization fields are grouped together in one authorization that only result in a valid authorization when together.

Authorization Object

An object in an SAP system. Makes the definition of authorizations possible in an SAP system. Comprises of upto 10 authorization fields that are connected with an AND link.

C

Cancellation workflow

Approval workflow that determines the approver when a requested product is canceled.

Cart

This is used to collect products in the IT Shop that can be requested at any time.
A customers can add as many carts as they want. The cart is deleted as soon as the requests contained in it have be carried out.

Cart item

A product that is assigned to a shopping cart.
A cart item makes it evident which product should be requested by whom for whom.

Central User Administration (CUA)

Function in SAP for administrating SAP user accounts in a central system rather than maintaining all clients separately.
SAP clients in different SAP system are grouped together in a system network. SAP user accounts for these SAP clients are maintained in a central system and the data is distributed to client systems. Therefore, users that own permissions in different SAP clients do not have to individually maintained. SAP roles and SAP profiles are administrated in client systems but can only be assigned to SAP user accounts in the central system.
Refer to your SAP system documentation for more details.

Company resource

Umbrella term for all objects that are assigned to employees or roles or that can be requested via the IT Shop and not roles themselves. Company resources are: applications, system entitlements, resources, target system groups, system roles.

Configuration parameter

Parameter for configuring the basic settings for Identity Manager system administration.
Preprocessor relevant configuration parameter are configuration parameters that are connected to a preprocessor condition. If a preprocessor relevant configuration parameter changes, the database has to completely recompiled.

Configuration Parameter Editor

Designer editor for customizing configuration parameters

Crypto Configuration

A program for encrypting the database contents of an Identity Manager database.

CUA

see Central User Administration (CUA)

CUA Status

Labels an SAP client for use as central system or client system in the central user administration. Clients that should be excluded from the Central User Administration are labeled with the CUA status ”None“.

Customer

A company employee that is entitled to request items from the IT Shop. An employee becomes a customer when assigned to a shop.
Customers form an IT Shop solution in combination with shelves, products, shops and shopping centers.

D

Database schema

A logical description of data that are saved in a database. The schema not only defines names for individual data items, their size and other characteristics, but also identifies the relation between the data.

The Identity Manager data model differentiates between reference data and metadata. Reference data is described by the application data model, the metadata by the interface data model.

Database Compiler

Program for compiling the Identity Manager database after changes have been made.

Database Installer

Program for installing and migrating an Identity Manager database.

Database Transporter

Program for exporting objects and custom changes from an Identity Manager database to an Identity Manager database.

DBQueue

Task list where triggered processing tasks are queued.

DBScheduler

The DBScheduler is used to calculate processing task from the DBQueue. The DBScheduler comprises of a combination of saved procedures and triggers.
The DBScheduler also controls recurring tasks on a cyclical basis such as daily maintainance tasks for calculating statistics or indexing the database.

Delegation

Special assignment request form
In the case, an employee passes any number of role assignments to another employee for a limited period of time. Delegations can be authorized via an approval procedure.

Designer

Main configuration interface for Identity Manager.

Discontinue inheritance

The property ”Discontinue inheritance“ indicates that the option ”End of inheritance“ is set in the master data of any role marked in this way.

Distribution model

Relationships between logical systems are defined in the SAP distribution model. It is used by Application Link Enabling to control data distribution amongst others.
Refer to your SAP system documentation for more details.

Domain Name System (DNS)

The Domain Name System (DNS) is a distributed database that manages namespaces in the internet.

Dynamic Host Configuration Protocol (DHCP)

Standard for administration of dynamic settings and addresses in a network. DHCP makes it possible to dynamically assign an IP address with the help of a DHCP server and other configuration parameters on computers in a network.

E

Enterprise Resource Planning (ERP)

Identifies the company task for planning the use of existing company resources in the most efficient way for daily operations.

Exception approver

A person that can approve rule exceptions.
Exception approvers are only those employees that are assigned to at least one compliance rule as exception approver via the application role <Identity Audit>\<Exception approver>.

F

Function Instance

Function definition that is given values for a specific application. A specific SAP client to be used in the SAP function is given in the function instance. Furthermore, variable that are allocated to authorization fields are given fixed values. Function instances can only be set up for active SAP functions.

Function Element

A general term for transactions, authorization objects and authorization fields that are displayed in an authorization definition as a tree structure in the Authorization Editor.

G

Business Role

Business roles represent customized functions in Identity Manager. You can use them to model approval workflows, assignments or approval procedures according to the needs of you organization structure. All business roles are specified by your company.

Global shelf template

Template that you can use to automatically generate shelves in all IT Shop shops.
A global shelf can be assigned company resources (as products) and approval policies.

H

HistoryDB

Archiving system for data changes.

HistoryDB Manager

Administration tool for displaying and editing all the information in the HistoryDB archiving system.

HistoryDB Service

System service on the servers. The HistoryDB Service imports log entries into the HistoryDB archiving system.

Hotfix

A hotfix contains corrections to the default configuration of the main installed version but no new functionality.

Hypertext Transfer Protocol (HTTP)

Protocol for transfering data.

I

Identity Manager (1)

Product for provisioning IT and other company resources.

Identity Manager (2)

Main administration tool for managing employees, user accounts and permissions within an Identity Manager network.

Identity Manager Service

A server system service. Identity Manager Service handling processing.

IT Shop (1)

Program component for providing employees with company resources via a defined approval procedure. IT Shop solutions are setup in Identity Manager and can then be used in the IT Shop.

IT Shop (2)

Web based application that provides various workflows.
In IT Shop you can change employee master data, edit employees, request company resources in the IT Shop, delegate roles, modify approvals, attestations or rule violations.

IT Shop Structure

Role classes are used to group the components of an IT Shop solution i.e. shopping center, shop, shelf, customer.

J

Job Queue Info

Programs for monitoring the current state of the services running in an Identity Manager network.

Job destination

Identity Manager Service component. The Job destination handles the process steps and returns the result back to the Job provider.

Job provider

Identity Manager Service component. A Job provider delivers process steps to the Job destination and evaluates the results.

Job queue

Central storage for process component generated actions to be executed.

Job server

Server running elementary tasks.

Job Server Editor

Designer for editing Job server properties.

Job Service Configuration

Program for configuring Identity Manager Service.

Job Service Updater

Program for updating Identity Manager Service on Job servers.

L

Language Editor

Designer Editor for translating text captions.

Lightweight Directory Access Protocol (LDAP)

Network protocol that permits queries and modifications to directory service's information (a hierical database distributed on a network).

List Editor

Designers basic editor with which list can be displayed and edited.

Lotus Notes

Document oriented distributed database system with a very tight email connection.

M

Manager

Main administration tool for displaying and editing all the information in an Identity Manager network.

Mapping

Maps target system object and their properties to database objects and their properties.
Mapping is used to synchronize data between the Identity Manager and target systems.

Mapping file

Contains extended rule for mapping properties between database and target system. The mapping file has an XML structure.
A mapping file can be created and extended with internal mapping rules for process components. Alternatively, a new mapping file can created that only contains extensions. If another extended mapping rule exists as a mapping file it is added to the process component internal mapping rule and the resulting rule is used to map the property.

Mitigating Control

A control that should be carried out if a compliance rule is violated or an SAP function matches. Mitigating controls are independent of Identity Manager functions. For example, the risk that is connected with a rule violation can be reduced by regular manual checking of prohibited authorizations.

N

NetBIOS

Network Basic Input Output System - Programmers interfaces developed by IBM to make communication between two network programs possible. NetBIOS allow 16 character for a NetBIOS name. Microsoft limited NetBIOS names to 15 characters because the 16th character is used as a NetBIOS suffix.

O

Object definition

Object definitions create a view for database objects that can be differated by their properties and therefore allow an additional control function.

Object Editor

Designers basic editor for displaying and editing all objects.

Organization

The company structures department, cost center and location are called organizations in Identity Manager.

Org level

An object in an SAP system that defines fixed values for authorization fields. Org levels are, for example, custom accounting codes, functional areas or account types.

P

Patch

Software update.

Permissions Editor

Designer editor used to grant table and column permissions to permissions groups and system users.

Plugin

Additional software module.

Preprocessor condition

Condition for posing restrictions on program code during compilation.
Conditional compilations allows parts of the program code to be included but excludes other parts. Preprocessor conditions are defined via configuration parameters and their options.

Process

Stringing together process step into a sensible order. The process has the task of mapping live processes.

Process Editor

Designer editor for handling process steps and processes.

Process function

Task executed by a process.

Process parameter

Parameter permitted for a single process component task.

Process step

Separate parts of a process. A process step represents one work procedure.

Process component

Elementary component available for use in process steps.

Product

Company resource that is assigned to an IT Shop shelf and therefore can be requested.
Products form an IT Shop solution in combination with shelves, customers, shops and shopping centers. Only company resources that are assigned to a service item and labeled with theoption <IT Shop> can be added as products to the IT Shop.

Provider client

The provider client is a completely configured Identity Manager customer environment with a database, Identity Manager Service and possibly Identity Manager front-ends. The provider client actively administers a network. In addition to the usual Identity Manager environment, the provider client can process its own Identity Manager Service requests that are executed on the provider master.

Provider master

The provider client is a completely configured Identity Manager provider environment with a database, Identity Manager Service and possibly Identity Manager front-ends. The provider master does not necessarily administer its own network but does however, contain additional information about the provider clients in its administration. The provider master keeps a queue for provider clients requests.

Provider mode

Provider mode is a model that stores and changes information in a central Identity Manager environment. The information is transfered into mainly independent Identity Manager environments and take effect there.

R

Release key

The release key is used by system users to change objects that are defined by Quest Software. The release key is only issued for a limited period of time and has to be specially requested.

Renewal workflow

Approval workflow that finds the approver if a requested product needs to be renewed.

Replication Info

Program for monitoring replication of software profiles.

Request template

Template for a cart containing cart items that are often requested together.
Public request templates are available to all Identity Manager users the moment they are shared. Non-public request templates can only be used by the request template owner.

Resource

An existing item for solving a particular task.

Resource type

Objects that are used to sort resources corresponding to usage.
Processing steps for resource types can be defined that need to be run when a resource is successfully assigned to an employee.

Role

The term ”role“ is an umbrella term for the company structures departments, cost centers, locations and business roles. Roles in Identity Manager are all objects though which employees, can be assigned company resources. Therefore IT Shop structures are also roles in the Identity Manager sense of the word.
Examples of roles are the department: ”Developement“, location ”Prague“, product ”FrameMaker - German - 9.0“.

Role classes

Objects that group together similar roles.
Role classes are defined in Identity Manager to differentiate between various company structures. Role classes regulate inheritance behavior in these company structures. Furthermore, they specify which company resource assignments are possible through a role in a role class.
Examples of role classes are: ”departments“, ”location“ or ”IT Shop structure“. Define custom role classes in order to create business roles.

Role type

Company specific criteria for allocating roles.
Role types are mainly used to regulate inheritance of approval policies within an IT Shop structure. To do this you define role types that you assign to the approval policies and IT Shop rules.
In addition, you can use role types to structure business role or shops in the IT Shop by criteria.

S

SAM Database

Security Accounts Manager - secure account administration under Windows.
Administration of user accounts and encoded password is done in the SAM database.

SAP Authorization

Authoriation permissions that that SAP user accounts obtain on the basis of the SAP roles assigned to them in the SAP system.

SAP Function

An object in Identity Manager that can be used to test which SAP authorizations an SAP user account in an SAP client has effectively.

SAP function category

An object for grouping SAP functions.

SAP menu

Element for guiding users through the SAP GUI. Authorizations are linked to fixed menu items with authorization objects. Authorization objects can be linked into authorization objects via the choice of SAP menu in the Identity Manager Authorization Editor.

SAP R/3

Product from the company SAP AG.

Schedule

Task to be performed on a cyclical basis.

Schedule Editor

Designer editor for setting up scheduled tasks for procedures that are to be executed cyclically.

Schema Extension

Program for extending the Identity Manager database schema with custom tables and columns.

Schema Editor

Designer editor for customizing database schema table and column definitions.

Secure Sockets Layer (SSL)

Transfer protocol that enables encoded communication.

Service catalog

Displays all requestable service items grouped by service category.
Service items for products that are assigned to IT Shop shelves are displayed in the service catalog.

Service category

Grouping criteria for service items
A product's service item must be assigned to a service category in order to select the product from the service catalog.

Service item

These are objects that are neccessary to book company resources internally.
Service items must be assigned to company resources so that they can be requested and booked internally as products in the IT Shop. A service item contains an exact product definition, assignment to a cost center, price information.

Service Pack

A service pack contains minor extension to the functionality and includes all changes since the last major version that were already included in hotfixes.

Service Provisioning Markup Language (SPML)

Service Provisioning Markup Language is an XML based description language that is used as an exchang format for user and resource information between provisioning systems. The standardization of SPML has been driven by the OASIS consortium (Organization for the Advancement of Structured Information Standards, www.oasis-open.org) which includes some well-known software companies. The lastest version (2.0) was released in April 2006.

Shelf

An IT Shop structure that is part of a shop and can be assigned products.
Shelves form part of a hierarchical IT Shop solution along with customers, shops, shopping centers and products.

Shelf template

Template that you can use to automatically generate shelves in IT Shop and fill them with company resources.
You can use shelf templates when you want to setup shelves in several shops with identical products. Identity Manager differentiates between global shelf templates, special shelf templates and shopping center templates.

Shop

An IT Shop structure that is assigned shelves and customers.
Shops form a hierarchical IT Shop solution along with customers, shelves, shopping centers and products. Each shop contains a shelves that the shop customer can request items from.

Shopping cart

See Cart.

Shopping center

IT Shop structure for group shops together.
Shops form a hierarchical IT Shop solution along with customers, shops, shelves and products.

Shopping center template

Template that you can user to replicate a shelf from a special shelf template in all the shops in a shopping center. To do this, the shopping center template must be assigned to at least one special shelf template.

Software Loader

Program for loading new or changed files in the Identity Manager database. They can then be distributed in the Identity Manager network through automatic software updating.

Special shelf template

Template that you can use to automatically generate shelves in selected shops in the IT Shop.
A special shelf template can be assigned company resources as products and approval policies. The shops that should be replicated by the shelf template are selected individually.

System role

A system role is a resource in which any number of company resources can be grouped together.
System roles are used to simplify assignment of different company resources. If a system roles is assigned to an employee , they receive all the company resources that are assigned to the system role. This might be system permissions, applications or non-IT Shop resources.
System roles can be assigned directly to employees, requested through the IT Shop or inherited through roles.

System user (1)

A predefined user that contains several entitlements to Identity Manager functions. The system user obtains these entitlements via his or her permissions groups assignments. A system user is assigned to user during the administration tool login procedure. Entitlements for the Identity Manager functions are passed onto the user from this system user.
Certain system users are included in the Identity Manager installation. Further system users can be defined in Designer.

System user (2)

An authentication module for logging onto Identity Manager tools. See Authentication module.

System user ID

The user ID that a user enters to log onto an Identity Manager tool.
The system user ID is independent of the selected authentication module. It can be a login name for an Active Directory domain or a system user e.g. a central user account.

T

Target system

A system in which employees under Identity Manager administration have access to network resources.
Example: Active Directory, SAP R/3, Lotus Notes

Target system area

Administration unit in a target system for user accounts, user groups and machine accounts.
Example: Active Directory domain, SAP R/3 client, Lotus Notes domain.

Template

Rule for mapping object properties. Templates can be used within an object as well as across objects.

Text comparison

A procedure in SAP which mirrors names of roles and profiles from a CUA client system in the central system. The roles and profiles in the central system are only made known when the text comparison has been run at least once. Then they can be assigned to user account.
Roles and profiles from client systems cannot be synchronized with Identity Manager until the text comparison has been run in SAP.
Refer to your SAP system documentation for more details.

Transaktion

An object in an SAP system that start an ABAP program.

U

UID

The UID is a artificial primary key that is created by the operating system as soon as the object is inserted in the database. The UID is a unique value which does not alter even when changes are made to the object properties. An object is labeled with a UID and can be uniquely referenced with it.

Unified Namespace (UNS)

Unified Namespace (UNS) is a virtual target system for mapping various target system along with their containers, user accounts, target system grous and associated memberships. The data for all target systems that are connected to Identity Manager is mapped in the Unified Namespace. This allows other core Identity Manager functions, such as compliance testing, attestation or IT Shop to be used across target system. The target systems Active Directory, Lotus Notes, SAP R/3 and LDAP can also mapped like your own applications, e.g. a telephone system.

User

The person that uses a tool to gain an advantage (a benefit such as time and/or cost reduction).

User account

Access entitlement to a restrictied access IT system. Normally users must authenticate themselves with a user name and password when logging in.

User & Permissions Group Editor

Designer editor for editing permissions groupa and system users.

User Interface Editor

Designers editor for editing the administration tool’s user interface.

V

Variable set

A group of all variables and their values that can be used in the authorization definition of an SAP function. Variable sets are used to set up fucntion instances for one and the same function definition.

Version update

A version update means significant additions to functionality and involves a completely new installation.

W

Windows Internet Name Service (WINS)

The Windows Internet Naming Service (WINS) is a software service developed by Microsoft that dynamically assigns IP addresses to computer names (NetBIOS names).

Workflow Editor

An editor that you can use to create workflows for attestation instances or approval processes.
In the Workflow Editor, approval levels and steps from an approval workflow are inserted via a special graphical control. Approval levels can be arranged in any way and connected to each other.

INDEX

A

Active Directory (AD)**483**
Active Directory account policy**255**
Active Directory contact
  assign groups**244**
  change container**241**
  contact data**243**
  delete**245**
  identification**244**
  inherit groups**241**
  lock**245**
  name**241**
  primary group**241**
  restore**245**
  setup**241**
Active Directory container
  application container**220**
  move**221**
  object class**220**
  organizational unit**220**
  setup**220**
  system container**220**
Active Directory domain
  account policy**208**
  domain name**210**
  domain type**206**
  LDAP account**211**
  logon**211**
  mapping file**209**, **263**
  mode**210**
  NetBIOS name**206**
  report**213**, **253**
  set up**206**
  synchronization server**210**, **263**
  trusted**212**
  user account resource**235**, **263**
Active Directory group
  distribution group**245**
  domain local**245**
  global**245**
  group scope**245**
  group type**245**
  security group**245**
  setup**246**
  universal**245**
Active Directory resource
  manage level**237**
Active Directory Service (ADS)**483**
Active Directory synchronization**204**
  access rights**203**
  configuration parameter**216**, **264**
  configure**215**, **265**
  unique sequence number**219**
Active Directory synchronization server
  configure**202**
  declaring**205**
  install**202**
  server hardware**205**
Active Directory user account
  account expiry date**222**
  account policy**225**
  administration**221**
  assign groups**234**
  automation level**287**
  callback option**230**
  change container**222**
  contact data**233**
  default PC**222**
  delete**239**
  home directory**227**
  identification**233**
  inherit application**222**
  inherit group**222**
  installation log**234**
  lock**239**
  login name**222**
  login period**229**
  login script**227**
  object class**222**
  password**225**
  primary group**222**
  profile directory**227**
  RAS dial-in**230**
  RAS dial-in data**230**
  retrieve**239**
  setup**222**

site**222**
terminal profile**231**
unlock**222**
user account resources**234**
workstation**229**
Application**483**
administration**123**
application type**124**
basic data**124**
delete**127**
dependency**127**
language**124**
operating system**124**
order of installation**127**
profile application**125**
section**125**
setup**124**
sort order**125**
Application group**483**
Application Link Enabling**483**
Application package
system role type**115**
Application packages
setup**127**
sharing**127**
Application role**62**, **483**
assign employees**69**
assign objects**68**
attestation administrator**472**
conflicting**70**
edit**68**
permissions group**62**
system user**62**
target system manager**70**
Applikationsserver**196**
Approval method**483**
Approval policy**483**
Approval procedure**483**
Approval workflow**483**
Approver**483**
Assignment
direct**76**
indirect**76**
primary**77**
secondary**78**
Assignment request**484**
Attestation**471**, **484**
approval method**479**
approval procedure**475**
approval methods**475**
approval workflow**482**
approval workflows**475**
attestation instance**481**
approval workflow**482**
attestation history**482**
closed attestion**481**
pending attestation**481**
time required**482**
attestation object**479**, **481**
attestation policy**475**
processing time**479**
attestation procedure**473**
Attestion instance**484**
attestion policy**479**
attestor**475**, **482**
define report**474**
schedule**479**
Attestion
attestor**484**
Authentication module**484**
role based**62**
system user**494**
Authorization definition
see SAP function > Authorization definition
Authorization editor**462**
see SAP function > Authorization editor
Authorization feld
see SAP function > Authorization definition > Authorization feld
Authorization object
see SAP function > Authorization object

B

Bootserver**196**
Business role**487**

C

Cancelation workflow**484**

Cart**484**
Cart item**485**
Central user administration**485**
Cluster Server**196**
  Homeserver**196**
Company IT data
  configuration parameter**33**
  determine**32**
  target system dependent**99**
Company resource**485**
Company resources
  assign**76**
Configuration parameter**485**
Configuration Parameter Editor**485**
Cost center
  company IT data**99**
  license node**94**
  setup**94**
Cost center structure**94**
Crypto Configuration**485**
CUA
  see Central User Administration
CUA status**485**
Customer**485**

D

Database Compiler**486**
Database Installer**486**
Database schedule
  viDynamicGroupCheck**102**
Database schema**180**, **485**
Database Transporter**486**
DBScheduler**486**
Default mail domain**31**
Default PC**47**
Delayed deletion**45**
Delegation**486**
Department
  assign**76**
  company IT data**99**
  license nodes**92**
  setup**92**
Department structure**92**
Dependencies
  mapping rule**190**
Designer**486**
Distribution model**486**
Domain
  Active Directory**206**
  initial filling**206**, **403**
  LDAP**403**
  master**206**, **403**
Domain Name System**486**
Domänencontroller**196**
Domino server
  declare**309**
Druckserver**196**
Dummy employee**53**
Dynamic Host Configuration Protocol**486**
Dynamic role
  calculate**103**

E

Employee
  administration**26**
  automatic assignment**40**
  central password**53**
  central user account**31**
  change**43**
  changing name**43**
  company IT data**32**
  data entry**46**
  default email address**31**
  default mail domain**31**
  default PC**47**
  delete**45**
  deputy**46**
  disable permanently**44**
  disable temporarily**44**
  dummy**53**
  external**47**
  general changes**43**
  ID card number**49**
  job rotation**43**
  leaving date**49**
  main identity**58**
  permanently disable**47**
  start date**49**

subidentity**58**
system user**53**
user account resource**37**
Employee assignment
automatic**40**
configure**41**
Mapping**42**
mode "Create"**41**
mode "No"**41**
mode "Search And Create"**41**
mode "Search"**41**
Enterprise Resource Planning**487**
Exception approver**432**, **487**
Exchange extensions
activate**277**, **291**
deactivate**277**, **291**
disable**288**
enable**288**
Extended property**424**
division limit**426**

F

Function category
see SAP function category
Function definition
see SAP function > function definition
Function element
see SAP function > authorization definition > Function element
Function instance
see SAP function > Function instance
Functional area**86**, **89**, **93**, **95**, **96**

G

Gateway Server**196**
Gateway server
configure**298**
declare**306**
install**298**
server hardware**306**
Group
Active Directory**246**
category**82**
LDAP**418**
Lotus Notes**330**
SAP R/3**383**
Unified Namespace**154**
Group membership
inherit**80**, **82**, **145**, **222**, **241**, **409**
limit**80**

H

HistoryDB**487**
HistoryDB Manager**487**
HistoryDB Service**487**
Homeserver**196**
Cluster Server**196**
Homeverzeichnis**196**
Hotfix**487**
Hypertext Transfer Protocol (HTTP)**488**

I

Identity Manager**488**
application role**62**, **483**
role model**61**
roles model**61**
user administration**29**
Identity Manager Service**488**
Inherit
group membership**241**
Inheritance
bottom-up**74**
category**82**
conditional**80**, **157**
discontinue**75**
group membership**145**, **222**, **409**
top-down**74**
Inheritance exclusion**157**
Inventoryserver**196**
IT Shop**488**
IT Shop structure**488**
Item**491**

J

Job destination**488**
Job provider**488**
Job queue**488**
Job server**488**
Job Server Editor**488**
Job Service Updater**489**

JobQueueInfo**488**

L

Language Editor**489**
LDAP domain
- authentication type**405**
- domain name**406**
- domain type**403**
- LDAP account**407**
- LDAP Store**406**
- login**407**
- mapping file**405**
- object class**406**
- port**405**
- provider**405**
- setup**403**
- synchronization server**406**
- user account policy**405**
- user account resource**413**

LDAP group
- delete**420**
- setup**418**

LDAP Store**196**, **403**
LDAP synchronization**402**
- accelerate**407**

LDAP synchronization server
- configure**401**
- declare**403**
- install**401**
- server hardware**403**

LDAP user
- administration**409**
- delete**417**
- disable**417**
- inherit applications**409**
- inherit groups**409**
- manage level**415**
- object class**409**
- retrieve**417**
- setup**409**
- user account resource**412**

Lightweight Directory Access Protocol (LDAP)**489**
List Editor**489**
Location
- assign**76**
- company IT data**99**
- license nodes**95**
- setup**95**

Location structure**95**
Lokaler ADS DC**196**
Lotus Notes**489**
Lotus Notes AdminP Request**312**
Lotus Notes certificate**314**
Lotus Notes domain
- mapping file**306**
- user account resource**325**

Lotus Notes group
- delete**334**
- group type**330**
- setup**330**

Lotus Notes lock group**332**
Lotus Notes server
- permissions type**339**
- server access**339**
- setup**335**
- type of restriction**339**

Lotus Notes synchronization**304**
- accelerate**310**
- procedure**296**

Lotus Notes templates**315**
Lotus Notes user
- address data**320**
- administration**315**
- certificate**317**
- delete**330**
- email system**319**
- lock**329**
- mail file**319**
- manage level**327**
- password**322**
- password policies**322**
- retrieve**330**
- setup**316**
- short name**317**
- unlock**329**
- user account resource**324**

user ID**323**
Lotus Notes user ID
expiry date**322**
renew**322**
restore**328**

M

Mail-enabled group**291**
alias**291**
approve membership**293**
disable**291**, **293**
display name**291**
dynamic distribution group**292**
email address**291**
enable**291**
expansion server**291**
Mail address**291**
moderated distribution group**293**
Mail-enabled recipient
addressing**289**
alias**289**
contact**288**
destination address**289**
destination address type**289**
disable**290**
display name**289**
enable**288**
recipient limitation**290**
user**288**
Mail-in database**334**
Manager**489**
Mapping**489**
Mapping file**180**, **489**
Mapping rule
customize**180**
database schema**180**
mapping file**180**
object type
dependencies**190**
schema file**180**
Master domain**206**, **403**
Master SQL Server**196**
Microsoft Exchange
administrative groups**268**
folder aministration policy**276**
folder structure**271**
global address list**273**
mailbox policy**274**, **276**
mailbox store**270**
mobile email query policy**274**
offline address list**273**
organization**267**
public folder**271**
share policy**276**
storage group**269**
user account resource**284**
Microsoft Exchange mailbox
addressing**278**
alias**278**
alternative recipient**278**
booking**282**
disable**283**
display name**278**
enable**277**
eqipment mailbox**277**
Equipment mailbox**282**
Legacy mailbox**277**
limits**281**
linked mailbox**277**
log settings**278**
mailbox store**278**
Mailbox type**277**
receiving restrictions**283**
Resource mailbox**277**
resource mailbox**282**
room mailbox**277**, **282**
setup**277**
shared mailbox**277**
size**281**
user account mailbox**277**
user account resources**284**
Microsoft Exchange recipient**276**
Microsoft Exchange Server**196**
Microsoft Exchange structure**267**
Microsoft Exchange synchronisation server
declare**263**
Microsoft Exchange synchronization**258**

access rights**259**
Microsoft Exchange synchronization server
configure**258**
declaring**261**
install**258**
Mitigating control**489**
assign automatically**429**
assign rule**429**
risk analysis**428**
SAP function**428**, **465**
assign**429**

N

NetBIOS**489**
NTFRS Basis**196**

O

Object definition**490**
Object Editor**490**
Org level
see SAP function > org level
Organization**490**

P

Password
central**53**
Password reset method**53**
Patch**490**
Plugin**490**
Preprocessor condition**490**
Procedure
viDynamicGroupCheck**102**
Process**490**
Process component**491**
mapping rule**180**
Process Editor**490**
Process function**490**
Process parameter**490**
Process step**490**
Profilserver**196**
Profilverzeichnis**196**
Property group**424**
Provider client**491**
Provider master**491**
Provider mode**491**
PXE Server**196**

R

Release key**491**
Renewal workflow**491**
Replication Info**491**
Request template**491**
Resource**105**, **491**
editing**106**
setup**108**
Resource package
setup**109**
system role type**115**
Resource type**491**
process step**107**
setup**106**
Rights Editor**490**
Risk analysis**86**, **89**, **93**, **95**, **96**
Role
assign**76**
business role**487**
dynamic**100**
license nodes**88**
organization**490**
setup**88**
user defined**492**
Role class**84**, **492**
direct assignment**78**
secondary assignment**78**
Role structure**88**
Role type**85**, **492**
Rule
compare**435**
compliance framework**423**
copy**438**
delete**448**
evaluation**450**
exception approval**432**
exemption approval**454**
Extended property**424**
IT Shop properties**436**
Property group**424**
property group**423**
rule condition**439**

rule group**423**
setup**430**
supervisor**432**
Rule base**423**
Rule checking
starting**449**
Rule condition
advanced**445**
employee group**442**
permissions**443**
permissions combination**443**
rule editor**440**
SAP function**447**
Rule editor**440**
Rule supervisor**432**
Rule violation**429**
mitigating control**428**

S

SAM database**492**
SAM Synchronisationsserver**196**
SAP
distribution model**486**
external ID
type
363
synchronizing central system**360**
SAP authorization**492**
SAP client
login data**352**
mapping file**354**
setup**352**
user account resource**375**
SAP company address**364**
SAP cost center**364**
SAP function**456**, **492**
Authorization definition
Function element**487**
authorization definition**462**, **484**
authorization feld**484**
authorization field**462**
edit status**462**
value**462**
variable**462**, **467**
Authorization Editor**484**
authorization editor**462**
authorization object**462**, **484**
copy variableset**469**
effect**461**
export**465**, **469**
function category**460**
function definition**461**
Function instance**487**
import**469**
manager**461**
mitigating control**428**
set up**465**
org level**467**, **490**
SAP menu**492**
set up**460**
severity level**461**
synchronization object**458**
transaction**462**, **495**
variable set**467**, **496**
add variable**469**
working copy**460**
create**466**
enable**465**
SAP function category**460**
SAP funktion category**492**
SAP group
administration**383**
SAP license**363**
value**363**
SAP login language**365**
SAP menu
see SAP function > SAP menu
SAP printer**364**
SAP product
system role type**115**
SAP profile
administration**383**
SAP R/3**492**
SAP R/3 synchronization**347**
permissions**346**
SAP role

administration**383**
SAP start menu**364**
SAP synchronization server
configure**344**
declare**348**
install**344**
server hardware**348**
SAP system
setup**349**
SAP system measurement**394**
SAP user
reference user**447**
SAP user account
address data**366**
communication**371**
defaults**372**
delete**380**
external identifier**382**
group memberships**380**
license information**394**
login data**369**
manage**361**
measurement data**394**
name**366**
password**369**
setup**365**
significance**396**
SNC name**373**
user account resource**374**
SAP user type**362**
Schedule**492**
Schedule Editor**492**
Scheduled task**103**
vi_PayLoadSchedule**104**
Schema Editor**493**
Schema Extension**493**
Schema file**180**
Secure Sockets Layer (SSL)**493**
see SAP function
synchronization object
Server
copy procedure**196**
setup**196**
Server function, in Identity Manager**196**
Service catalog**493**
Service category**493**
Service item**493**
Service Pack**493**
Service Provisioning Markup Language**493**
Shelf**493**
Shelf template**493**
global**487**
shopping center template**494**
special**494**
Shop**493**
Shopping cart
see Cart
Shopping center**494**
SMTP Host**196**
Software Loader**494**
Sychronization
SAP R/3
Restrict synchronization objects**360**
Synchronisation by Identity Manager**162**
Synchronisationsserver**196**
Synchronization**161**
Active Directory**204**
LDAP**402**
Lotus Notes**304**
Microsoft Exchange**258**
post processing**176**
SAP function**458**
SAP R/3**347**
target system reconciliation**176**
Synchronization configuration
prerequisites**162**
setup**163**
System role**105**, **114**, **494**
edit**115**
System role type**115**
Application package**115**
resource package**115**
SAP product**115**
System user**61**, **494**
authentication module**494**
System user ID

definition**494**

T

Target system**494**
Target system mananger**70**
Target system reconciliation**176**
Target system wizard**205**, **305**, **347**
Target system zone**495**
Task
scheduled**103**
Template**495**
Text comparison**495**
Transaction
see SAP function > Transaction

U

UID**495**
Unified Namespace**131**, **495**
authorization element**140**
configure**135**
target system manager**70**
user account resource**149**
Unified Namespace container**141**
Unified Namespace group**154**
Unified Namespace user account
inherit group**145**
manage level**152**
setup**145**
user account resource**148**
Unique sequence number**219**
UNS**495**
User account
administration**26**
assign employee (automatically)**40**
automation level**26**, **287**
category**82**
central**31**
company IT data**32**
disable**45**
full managed**26**
linked**26**
manage level**237**
restore**45**
status**26**
unlinked**26**
unmanaged**26**
user account resource**37**
User account resource**37**
automation level**287**
create (Active Directory)**235**
create (LDAP)**413**
create (Lotus Notes)**325**
create (Microsoft Exchange)**284**
create (SAP R/3)**375**
create (Unified Namespace)**149**
default manage level**37**
levels**237**
manage level**37**, **237**, **287**, **377**
User account resources**45**
User category
SAP**354**
User Interface Editor**495**
Users and Permissions Group Editor**495**

V

Variable set
see SAP function > Variable set
Version update**496**
VIAgentsDB.NSF**303**
VINotes.INI**303**

W

Windows Internet Name Service**496**
Workflow Editor**496**